DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

VERSIÓN PÚBLICA

DIRECCIÓN GENERAL DE REPOSITORIOS UNIVERSITARIOS
UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO |

Fecha de aprobación: agosto 2022

Contenido

OBJETIVO GENERAL

Este documento es un instrumento que tiene por objetivo describir y dar cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee la Dirección General de Repositorios Universitarios (DGRU), es decir, describe el conjunto de elementos y actividades que conforman el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

OBJETIVO PARTICULAR

Reducir el riesgo de vulneraciones a los datos personales y el número de personas que tratan datos personales a las mínimas indispensables.

ABREVIATURAS

CDI: Colecciones y Datos de Investigación

DG: Dirección General

DGRU: Dirección General de Repositorios Universitarios

DTI: Desarrollo Tecnológico e Infraestructura

PGN: Planeación, Gestión y Normatividad

SRU: Sistema de Repositorios Universitarios

ALCANCE

Este documento es aplicable a todos los datos personales a los que el personal de la DGRU realice tratamiento, entendiendo este como: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

DEFINICIONES

Activo [1]

Todo elemento de valor para la Universidad, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

Activo crítico

Todo elemento de valor para la DGRU, involucrado en el tratamiento de datos personales.

Contenedor.

Medio, físico o técnico, en el que se registra y guarda el activo.

Contenedor físico.

Medio tangible en el cual se almacena el activo, al que se accede sin intervención de algún dispositivo electrónico. Por ejemplo: expedientes ubicados en libreros.

Contenedor técnico.

Medio en el cual se almacena el activo, al que se accede sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos. Por ejemplo: carpetas digitales ubicadas en un servidor virtual, internet, discos ópticos (CDs, DVDs), espacio encriptado de la DGRU, unidad de almacenamiento, entre otros.

Encargado [1]

La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

Medidas de seguridad [1]

Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales.

Recursos humanos.

Personas responsables o encargadas del tratamiento de datos personales de un activo de la DGRU.

Responsable [1]

Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

Sistema de Gestión de Seguridad de Datos Personales [1]

Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales

Sistema de tratamiento de datos personales [1]

Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos

[1] Universidad Nacional Autónoma de México (30 de enero de 2020). Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad. Gaceta UNAM. Núm. 5112. Gobierno, pp. 22-28.

FUNDAMENTO

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos— en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

El presente documento de seguridad, se fundamenta específicamente en los artículos 31, 32 y 33 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019 y en las Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección

de datos personales en posesión de la Universidad, publicado en la Gaceta UNAM el 30 de enero de 2020.

POLÍTICA

Proteger los datos personales a los que da tratamiento la DGRU, en cumplimiento con la legislación Universitaria vigente en materia de protección de datos personales y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

FUNCIONES Y RESPONSABILIDADES

Las funciones y responsabilidades, así como la cadena de rendición de cuentas del personal que trata los datos personales en la DGRU se describen de manera específica en cada activo, en los Anexos 1 al 10.

A nivel general la DGRU cuenta con dos responsables de seguridad de datos personales: el coordinador de DTI y la coordinadora de PGN. Con respecto a la elaboración del Sistema de Seguridad de Datos Personales se establece la siguiente relación entre funciones y responsables:

Función	Coordinadora de PGN	Coordinador de DTI	Coordinador de SRU	Coordinador de CDI	Directora General
Definir el Alcance	X	X			X
Definir Objetivos	X	X			X
Definir Política	X	X			X
Definir Funciones y Obligaciones	X	X	X	X	X
Elaborar el Inventario de Datos Personales	X	X	X	X	
Realizar el análisis de riesgo de los Datos Personales	X	X	X	X	
Realizar el análisis de Brecha de las Medidas de Seguridad	X	X	X	X	
Implementar las Medidas de Seguridad Aplicables a los Datos Personales	X	X	X	X	X
Capacitar	X	X			
Revisar y auditar internamente					X

LISTADO DE ACTIVOS

La DGRU cuenta con los siguientes activos:

IJ1 Instrumentos jurídicos de la DGRU
Documentos que sirven de sustento en convenios o bases de colaboración que se firman con entidades académicas, dependencias universitarias o instituciones externas a la universidad.

PE1 Apoyo de gestión administrativa del personal
Documentos relacionados con la contratación del personal que se realiza ante la unidad administrativa de la Secretaría de Desarrollo Institucional, o para cuando existe un proceso de gestión con respecto a los bienes de la dependencia.

PE2 Gestión sanitaria y emergencias
Información para atender la comunicación necesaria en caso de una emergencia y para registrar datos conforme a las disposiciones del Comité de Seguimiento COVID-19, UNAM.

DG1 Contraseñas de gestión administrativa
Documentos relacionados con el acceso a sistemas de la UNAM externos a la DGRU para realizar actividades de gestión administrativa.

DG2 Formatos de gestión interna
Documentos de gestión interna relacionados con las actividades sustantivas de la DGRU, como minutas,formatos de registro de capacitación y de atención a usuarios.

DG3 Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
Grabaciones y documentos relacionados con la autorización para el uso de imagen o voz personales y contenidos, que se utilizan para contactar a las personas asistentes a los eventos.

SRU1 Repositorio Institucional de la UNAM
Metadatos de los contenidos digitales integrados en la plataforma digital: Repositorio Institucional de la UNAM.

CDI1 Portal de Datos Abiertos UNAM, Colecciones Universitarias
Metadatos de los contenidos digitales integrados en la plataforma digital: Portal de Datos Abiertos UNAM, Colecciones Universitarias e información de curadores para su acceso a la plataforma.

DTI1 Correo electrónico
Correos electrónicos con datos personales que se usan en comunicaciones para el apoyo en la gestión de procesos internos y el ejercicio de las actividades sustantivas de la DGRU. La comunicación puede ser a través de las cuentas de correo electrónico: contacto@dgru.unam.mx, archivo@dgru.unam.mx, ayuda@dgru.unam.mx, contacto@repositorio.unam.mx y todas las cuentas institucionales del personal que labora para la DGRU con dominio @dgru.unam.mx o @ccud.unam.mx.

DTI2 Cámaras de seguridad
Grabaciones de las instalaciones de la Dirección General de Repositorios Universitarios para procurar la seguridad de las personas e instalaciones.

ELEMENTOS ANALIZADOS POR CADA ACTIVO

Cada uno de los activos anteriormente mencionados, se describieron conforme a los siguientes elementos:

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

Describe los datos personales contenidos en el activo en cuestión, cómo se obtienen, para qué se usan, se especifica si los datos son transferidos, donde se alojan y cuánto tiempo se da tratamiento. También contiene la lista de personas responsables y encargadas de dar tratamiento a los datos personales.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

Identifica el tipo de soporte: físico o electrónico, donde se alojan los datos personales y sus características principales.

3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN.

Identifica el activo crítico, la razón por la cual se seleccionó, se proporciona una breve descripción, se indica a quién pertenece el activo de información, cuáles son los requisitos de seguridad para el activo y se señala el requisito de seguridad más importante.

También se elaboraron los mapas de ambientes de riesgo del activo, en los cuales se identifica el tipo de contenedor que puede ser técnico (ej. carpetas electrónicas alojadas en un servidor virtual) o físico (ej. libreros), y recursos humanos, es decir, personas que tienen alguna función o responsabilidad con respecto al activo, se señala el área a la que pertenecen y se identifica tanto a contenedores como al personal interno y externo a la DGRU, este último aplica en el caso de que el activo sea remitido o transferido.

4. RIESGO DE ACTIVO DE INFORMACIÓN.

Se identificaron las áreas de preocupación para el activo, es decir las acciones que pueden afectar la seguridad de los datos personales.

Para cada contenedor del activo y los recursos humanos involucrados, se identificaron distintos escenarios de riesgo, es decir situaciones en las que el activo pudiera ser expuesto a personal no autorizado, modificado, interrumpido o destruido de manera que se vuelve inutilizable para los propósitos legítimos.

5. ANÁLISIS DE RIESGOS.

Estudio que se realiza considerando el riesgo que tiene la información (o área de preocupación) y el impacto de su ocurrencia (ver Anexo 11) para señalar las medidas aplicadas y por aplicar para mitigar el riesgo.

- Los escenarios de amenazas para los activos, señalando los medios por los cuales alguna persona podría explotar alguna debilidad en el activo, cuál sería el efecto sobre el activo (alteración, eliminación, divulgación) cómo serían violados los requisitos de seguridad del activo y la probabilidad de que la amenaza ocurra.

- Criterios de medición del riesgo, es decir, se identifican qué tan graves son las consecuencias para la DGRU o para el propietario del activo por área de impacto. Las áreas de impacto consideradas son: reputación y confianza, seguridad y salud, productividad, financiera y medidas de apremio y sanciones (ver Anexo 11). De acuerdo al riesgo que tiene la información, en esta misma etapa se establecen las medidas que se tomarán, es decir, aceptar, aplazar, mitigar o transferir el riesgo. En los

casos en donde se haya decidido mitigar el riesgo, se indican los controles aplicados y por aplicar para cada contenedor y se señalan los riesgos residuales que serían aceptados.

6. ANÁLISIS DE BRECHA.

Diagnóstico que permite identificar las medidas de seguridad existentes; las medidas de seguridad necesarias, las acciones para lograr el nivel de seguridad óptimo y los requerimientos para alcanzar dicho nivel.

7. PLAN DE TRABAJO.

Describe las actividades, objetivos y el impacto que tienen en la protección de datos personales, así como su duración, cobertura y prioridad.

8. MEDIDAS DE SEGURIDAD.

Describe las medidas implementadas o por implementar para garantizar la seguridad de los datos personales durante la transferencia de información. Considera:

I. Si la transferencia se puede realizar a través de soportes físicos, electrónicos o sobre redes electrónicas.

II. Las medidas de seguridad que se han implementado para el resguardo de los sistemas de tratamiento con soportes físicos, teniendo en cuenta las medidas implementadas para evitar que los datos personales puedan ser alterados, extraviados o que haya acceso no autorizado, así como los nombres, cargos, funciones y obligaciones de las personas que pueden acceder a dichos soportes físicos.

III. Las bitácoras para acceso y operación cotidiana. En caso de que se lleve el control a través de estas bitácoras, se especifican los datos que se registran, por ejemplo para los soportes físicos, el nombre de las personas que acceden a los datos personales, fecha y hora en que se realiza el acceso, el propósito de acceder a la información; si se utiliza alguna herramienta informática y para los soportes electrónicos se describen las medidas aplicadas y por aplicar para llevar el control a través de bitácoras y se señala quién es responsable de analizar dichas bitácoras.

IV Registro de incidentes. Describe las medidas aplicadas y por aplicar para contar con un procedimiento de atención a incidentes, señala la información que se debe incluir en el reporte del incidente, la persona que lo resuelve, la metodología que se aplica, las

medidas en caso de que el incidente se haya presentado en soportes físicos o soportes electrónicos, incluyendo cómo se asegura la integridad de los reportes y en caso de que sea necesario, quién autoriza la recuperación de la información de los soportes físicos.

V. Acceso a las instalaciones. Describe las medidas de seguridad perimetral exterior e interior implementadas y por implementar para las instalaciones y para el acceso del personal.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales. Señala el procedimiento institucional para actualizar la información personal contenida en el sistema.

VII. Perfiles de usuario y contraseña. Describe el esquema de perfiles de usuario y contraseña implementados para control de acceso mediante una red electrónica, detallando el modelo de control de acceso, los perfiles de usuario y contraseñas en el sistema operativo de red, los perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales, se detalla cómo es la administración de perfiles de usuario y contraseñas; finalmente se detalla cómo es el acceso remoto al sistema de tratamiento de datos personales.

VIII. Procedimientos de respaldo y recuperación de datos. Indica si se realizan respaldos, si se hace de manera manual o automática y la periodicidad; los medios en que se almacenan las copias de seguridad, cómo, dónde se archivan esos medios y quién es el responsable de realizarlos.

IX. Plan de contingencia. Establece el plan implementado para garantizar la continuidad de la operación del sistema, señala si se realizan pruebas de su eficiencia y en caso de contar con un sitio redundante alterno, señala sus características. el personal que lo pone en marcha y el tiempo que se requiere para que esté en marcha dicho sitio.

9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Describen las herramientas o recursos empleados para monitorear la protección de datos personales, indicando el tipo de herramienta que se emplea, la forma en que se controla y se verifica el uso de dicha herramienta; el procedimiento para revisar las medidas de seguridad, el responsable de realizar el procedimiento. el tiempo máximo de ejecución; comunica los resultados de la evaluación y pruebas de las medidas de seguridad y las acciones para la corrección y actualización de dichas medidas.

10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN.

Describe las actividades planteadas para la capacitación de las personas responsables de seguridad de datos personales, su duración, el público objetivo, vigencia y frecuencia, así como la prioridad de cada actividad. De igual manera, incluye las actividades planteadas para la capacitación del personal de la DGRU, duración, cobertura, así como la prioridad de las actividades.

MEDIDAS DE SEGURIDAD TÉCNICAS

Los activos con contenedores técnicos están relacionados con plataformas a los que es necesario aplicar las Medidas de Seguridad Técnicas, siguiendo la ruta crítica que la Universidad ha proporcionado para su cumplimiento. Dada la extensión de las mismas y el número de sistemas involucrados, se concentran en el Anexo 12 las acciones realizadas para su cumplimiento en términos de los artículos que la normatividad lo señala.

MEJORA CONTINUA Y CAPACITACIÓN

Para efectos de mejora continua, posterior a las revisiones y auditorías, se revisan los hallazgos, acciones correctivas y preventivas, así como se actualiza el programa específico de capacitación que corresponda.

Para concientizar al personal de la DGRU sobre el adecuado tratamiento de datos personales y dar a conocer el sistema de gestión de seguridad de datos personales, se lleva a cabo un programa de difusión y capacitación que incluye las siguientes acciones:

- Elaboración de presentaciones
- Sesiones de capacitación
- Envío de correos electrónicos con información del tema y material de apoyo
- Atención y respuesta a dudas específicas vía correo electrónico, videoconferencia o presencial
- Invitaciones a capacitaciones y eventos externos a la DGRU relacionados con la materia.

El programa de difusión y capacitación abarca principalmente los siguientes temas:

1. Breve explicación del contexto
2. Conceptos y figuras en el tratamiento de datos personales

3. Figuras en el tratamiento de datos personales
4. Sistema de Información
5. Principios del tratamiento de datos personales
6. Obligaciones del encargado
7. Remisiones
8. Transferencias de datos personales
9. Facultad de verificación
10. Procedimiento de verificación
11. Medidas de apremio
12. Sanciones
13. Normatividad institucional UNAM
14. Normatividad DGRU
15. Sistema de Gestión de Seguridad de Datos Personales
16. Buenas prácticas para equipos de cómputo y dispositivos portátiles
17. Buenas prácticas para documentos y correos electrónico
18. Buenas prácticas dentro de las instalaciones de la DGRU
19. Disposición y consulta de documentos físicos
20. Buenas prácticas para alta de personal
21. Buenas prácticas para baja de personal
22. Reporte de incidentes de vulneración de datos personales

ANEXOS

Anexo 1	IJ1 Instrumentos jurídicos de la DGRU
Anexo 2	PE1 Apoyo de gestión administrativa del personal
Anexo 3	PE2 Gestión sanitaria y emergencias
Anexo 4	DG1 Contraseñas de gestión administrativa

Anexo 5	DG2 Formatos de gestión interna
Anexo 6	DG3 Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
Anexo 7	SRU1 Repositorio Institucional de la UNAM
Anexo 8	CDI1 Portal de Datos Abiertos UNAM, Colecciones Universitarias
Anexo 9	DTI1 Correo electrónico
Anexo 10	DTI2 Cámaras de seguridad
Anexo 11	Criterios de medición del riesgo
Anexo 12	Medidas de Seguridad Técnicas (MST)

CONTROL DE CAMBIOS

No aplica.

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

APROBACIÓN

Elaboración: Responsables de seguridad de datos personales de la DGRU y Responsables de áreas	M. en C. Ariana Chávez Méndez Coordinadora de Planeación, Gestión y Normatividad ariana.chavez@dgru.unam.mx	C. Omar Alejandro Solís Garza Coordinador de Desarrollo Tecnológico e Infraestructura omar.solis@dgru.unam.mx
Revisión: Responsables de áreas	Lic. en C. C. Rubén Ignacio Sáenz González Coordinador del Sistema de Repositorios Universitarios ruben.saenz@dgru.unam.mx	M. en C. Oliver Joaquín Giménez Heáu Coordinador de Colecciones y Datos de Investigación joaquin@dgru.unam.mx
Aprobación: Titular de la DGRU	Dra. Tila María Pérez Ortiz Directora General de Repositorios Universitarios tilam@dgru.unam.mx	
Fecha de aprobación:	Agosto 2022	
Fecha de actualización:		

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

De conformidad con la **Resolución: CTUNAM/529/2022** emitida por el Comité de Transparencia de la Universidad Nacional Autónoma de México el 24 de agosto de 2022, se reservan las siguientes secciones del documento de seguridad, para cada activo de la DGRU:

1. Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa);
2. Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información;
3. Diagramas de Arquitectura;
4. Análisis de Riesgos;
5. Análisis de Brecha;
6. Plan de Trabajo;
7. Política de Autenticación y Control de Acceso;
8. Política de seguridad física;
9. Medidas de seguridad implementadas;
10. Mecanismos de monitoreo y revisión de medidas de seguridad;
11. Políticas de Respaldos, y
12. Medidas de Seguridad Técnicas.

Lo anterior con base en las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, el Comité de Transparencia CONFIRMA la **reserva** total de una parte de la información para la elaboración de la versión pública, por un periodo de **cinco años**, que se computarán a partir de la fecha de la resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

Anexo 1. IJ1 Instrumentos jurídicos de la DGRU

1.1 INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
Datos personales (sensibles o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: Nombre. 1b. Datos laborales: Puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional. 1c. Datos académicos: Títulos.	
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X)	
¿Para qué se usan?	Los datos personales señalados se utilizan para complementar la información requerida en los convenios, bases de colaboración con dependencias o entidades universitarias o con instituciones externas a la universidad.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal (X)	Gobierno Estatal ( ) Gobierno Municipal ( ) Personas físicas (X) Personas morales ( ) Áreas Universitarias (X) Para la elaboración, validación o resguardo de Convenios o Bases de Colaboración.

¿Dónde se alojan?	[redacted]
¿Cuánto tiempo se da tratamiento?	El tiempo del periodo desde que se elaboran, revisan y validan las bases o convenios de colaboración, hasta la vigencia de los mismos. Terminada la vigencia, la disposición de los instrumentos jurídicos y periodo de resguardo estará sujeto a lo establecido en los Instrumentos de Control y Consulta Archivística de la UNAM vigentes.
Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación
Funciones:	Recabar y comunicar la información personal relacionada con los instrumentos jurídicos.
Obligaciones:	Una vez recabados los datos personales, se integran al instrumento jurídico de que se trate (bases o convenios de colaboración) y se envía dicho instrumento jurídico a las entidades universitarias, dependencias universitarias o instituciones externas que suscriben el instrumento, una vez suscrito, se digitaliza y almacena en un espacio encriptado de la DGRU, el documento físico se resguarda conforme a los Instrumentos de Control y Consulta Archivística de la UNAM y en algunos casos se deposita en la Oficina de la Abogacía General de la UNAM conforme a la normativa universitaria.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Rubén Ignacio Sáenz

Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Recabar y comunicar la información personal relacionada con los instrumentos jurídicos.
Obligaciones:	Una vez recabados los datos personales, se integran al instrumento jurídico de que se trate (bases o convenios de colaboración) y se envía dicho instrumento jurídico a las entidades universitarias, dependencias universitarias o instituciones externas que suscriben el instrumento, una vez suscrito, se digitaliza y almacena en un espacio encriptado de la DGRU, el documento físico se resguarda conforme a los Instrumentos de Control y Consulta Archivística de la UNAM y en algunos casos se deposita en la Oficina de la Abogacía General de la UNAM conforme a la normativa universitaria.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Recabar y comunicar la información personal relacionada con los instrumentos jurídicos.
Obligaciones:	Una vez recabados los datos personales, se integran al instrumento jurídico de que se trate (bases o convenios de colaboración) y se envía dicho instrumento jurídico a las entidades universitarias, dependencias universitarias o instituciones externas que suscriben el instrumento, una vez suscrito, se digitaliza y almacena en un espacio encriptado de la DGRU, el documento físico se resguarda conforme a los Instrumentos de Control y Consulta Archivística de la UNAM y en algunos casos se deposita en la Oficina de la Abogacía General de la UNAM conforme a la normativa universitaria.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad

Funciones:	Recabar y comunicar la información personal relacionada con los instrumentos jurídicos.
Obligaciones:	Una vez recabados los datos personales, se integran al instrumento jurídico de que se trate (bases o convenios de colaboración) y se envía dicho instrumento jurídico a las entidades universitarias, dependencias universitarias o instituciones externas que suscriben el instrumento, una vez suscrito, se digitaliza y almacena en un espacio encriptado de la DGRU, el documento físico se resguarda conforme a los Instrumentos de Control y Consulta Archivística de la UNAM y en algunos casos se deposita en la Oficina de la Abogacía General de la UNAM conforme a la normativa universitaria.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Ana Laura Méndez Franco
Cargo:	Jefa del Departamento de Planeación y Seguimiento de Proyectos
Funciones:	Revisar que se mantenga la integridad de los datos personales en los documentos relacionados con el proceso de elaboración, validación y resguardo de las bases o convenios de colaboración.
Obligaciones:	Durante todo el proceso de elaboración, validación y resguardo de las bases o convenios de colaboración se asegura de que los documentos relacionados sean clasificados y archivados de manera correcta de acuerdo con los procedimientos internos de la DGRU y de acuerdo a los Instrumentos de Control y Consulta Archivística de la UNAM, así como de que se mantenga la integridad de los datos personales contenidos en los instrumentos jurídicos.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Responsable	
Nombre:	Edurne Dolores Uriarte Santillán

Cargo:	Jefa del Departamento de Inventario de Colecciones y Datos de Investigación
Funciones:	Recabar y comunicar la información personal relacionada con los instrumentos jurídicos.
Obligaciones:	Una vez recabados los datos personales, se integran al instrumento jurídico de que se trate (bases o convenios de colaboración) y se envía dicho instrumento jurídico a las entidades universitarias, dependencias universitarias o instituciones externas que suscriben el instrumento, una vez suscrito, se digitaliza y almacena en un espacio encriptado de la DGRU, el documento físico se resguarda conforme a los Instrumentos de Control y Consulta Archivística de la UNAM y en algunos casos se deposita en la Oficina de la Abogacía General de la UNAM conforme a la normativa universitaria.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Encargados	
Nombre:	Alejandro Chávez Méndez
Cargo:	No Aplica
Funciones:	Resguardar de manera segura los datos personales contenidos en los documentos físicos y digitales relacionados con el proceso de elaboración, validación y resguardo de las bases o convenios de colaboración.
Obligaciones:	Digitalizar los instrumentos jurídicos que contienen los datos personales, asegurando la integridad de dichos datos personales. Archivar el documento digital en un espacio encriptado en la DGRU. Archivar el documento físico conforme a los Instrumentos de Control y Consulta Archivística de la UNAM y en algunos casos se deposita en la Oficina de la Abogacía General de la UNAM conforme a la normativa universitaria. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Usuarios	

Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

1.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	IJ1
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU
Tipo de soporte:	[redacted].
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]

[redacted]

1.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Instrumentos Jurídicos (Bases de Colaboración, Convenios Generales, Convenios Específicos)	Los instrumentos son el fundamento legal para la colaboración entre entidades y dependencias universitarias así como con entidades externas con la DGRU. Los instrumentos contienen datos personales protegidos por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	Son acuerdos consensuales entre dos partes para colaborar bajo lineamientos definidos. Estos instrumentos contienen datos personales relacionados con los representantes de las partes que los suscriben.
Dueño		
¿A quién pertenece el activo de información?		
Directora General		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
( ) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente manera:	Los documentos son susceptibles de ser extendidos mediante la adición de documentos, únicamente por personal del área responsable.
(X) Disponibilidad	Este activo debe estar disponible para que el personal	La versión digital del documento está

	realice sus labores de la siguiente manera:	disponible para consulta previa solicitud mediante correo electrónico. El documento físico está disponible para consulta previa justificación autorizada por la Coordinadora de Planeación, Gestión y Normatividad.
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
( ) Confidencialidad	**(X) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	

1.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Instrumentos jurídicos de la DGRU
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

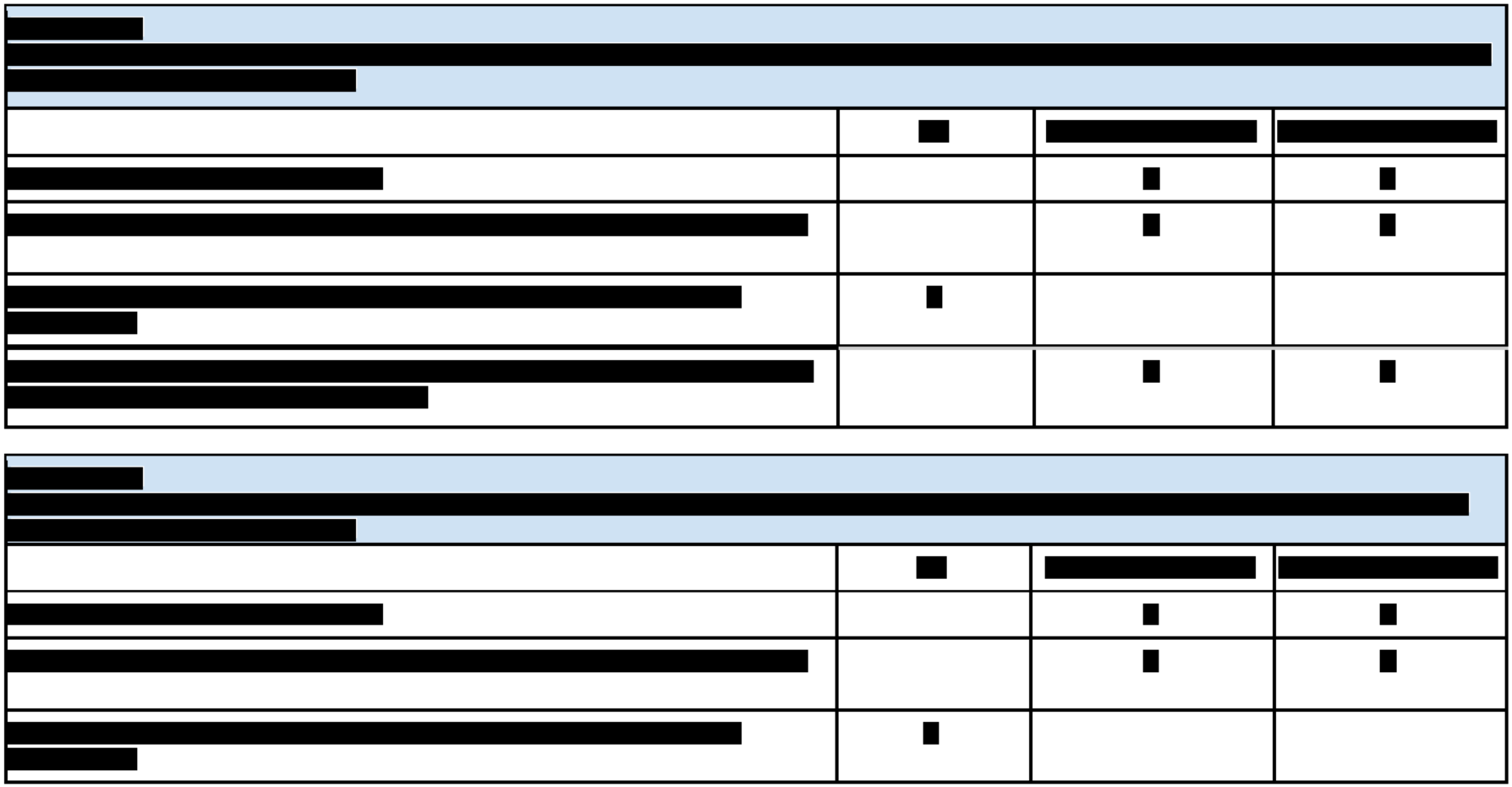
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]			
[redacted]			

[redacted]		[redacted]	[redacted]

[redacted]					
[redacted]				[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]			[redacted]	[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]			[redacted]	[redacted]	[redacted]

CONTENEDORES FÍSICOS



[redacted]

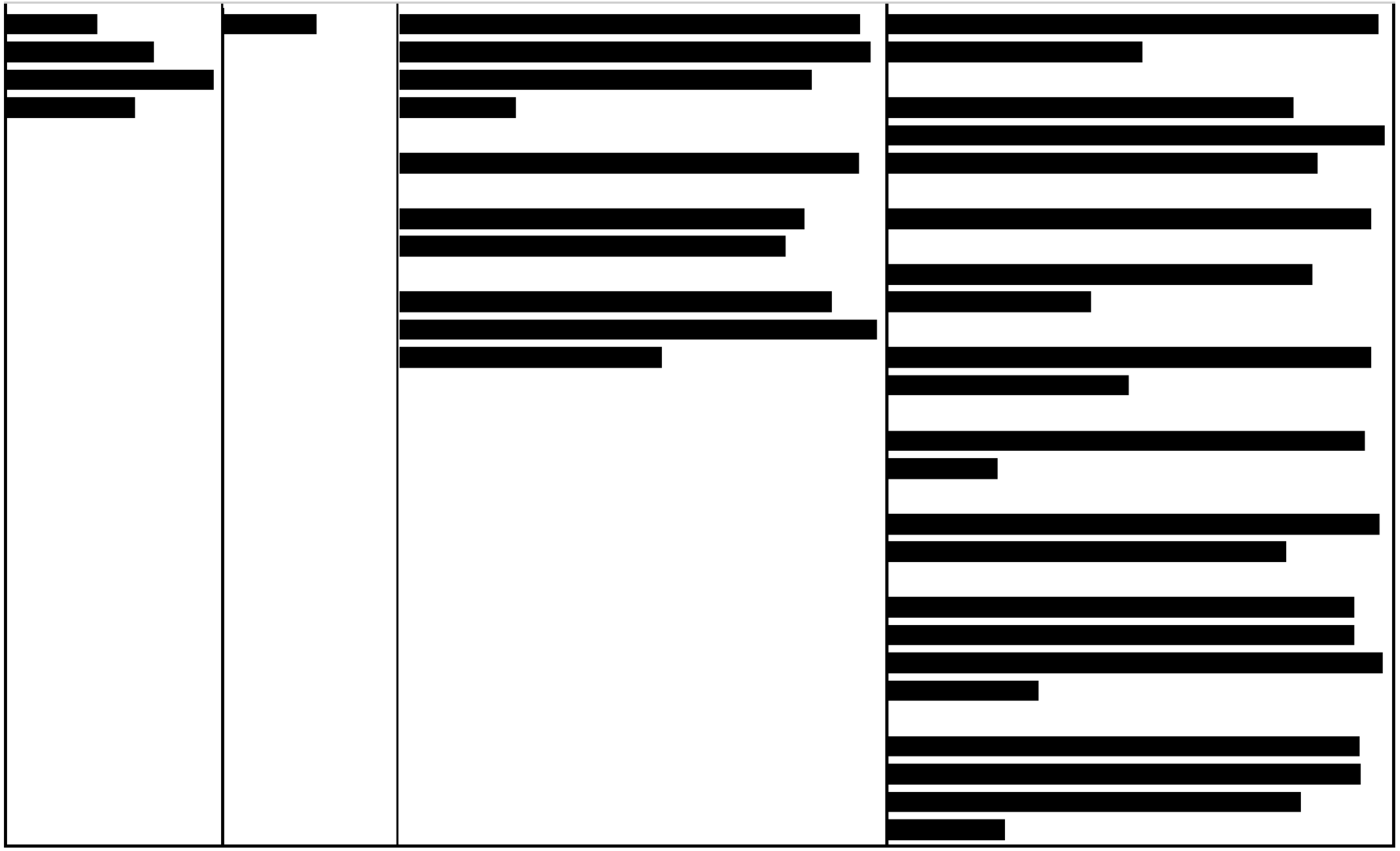
[redacted]

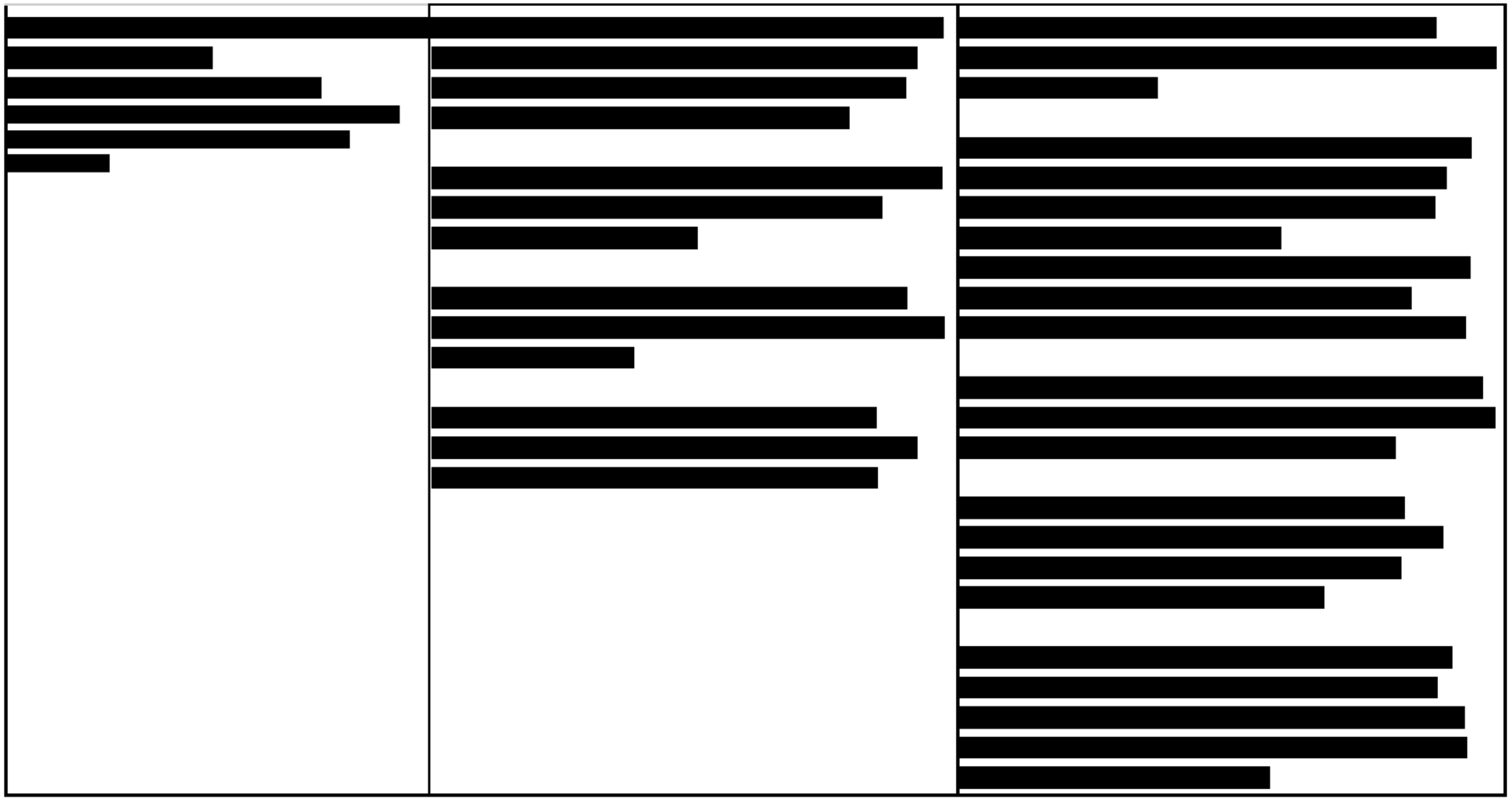
RECURSOS HUMANOS

[redacted]

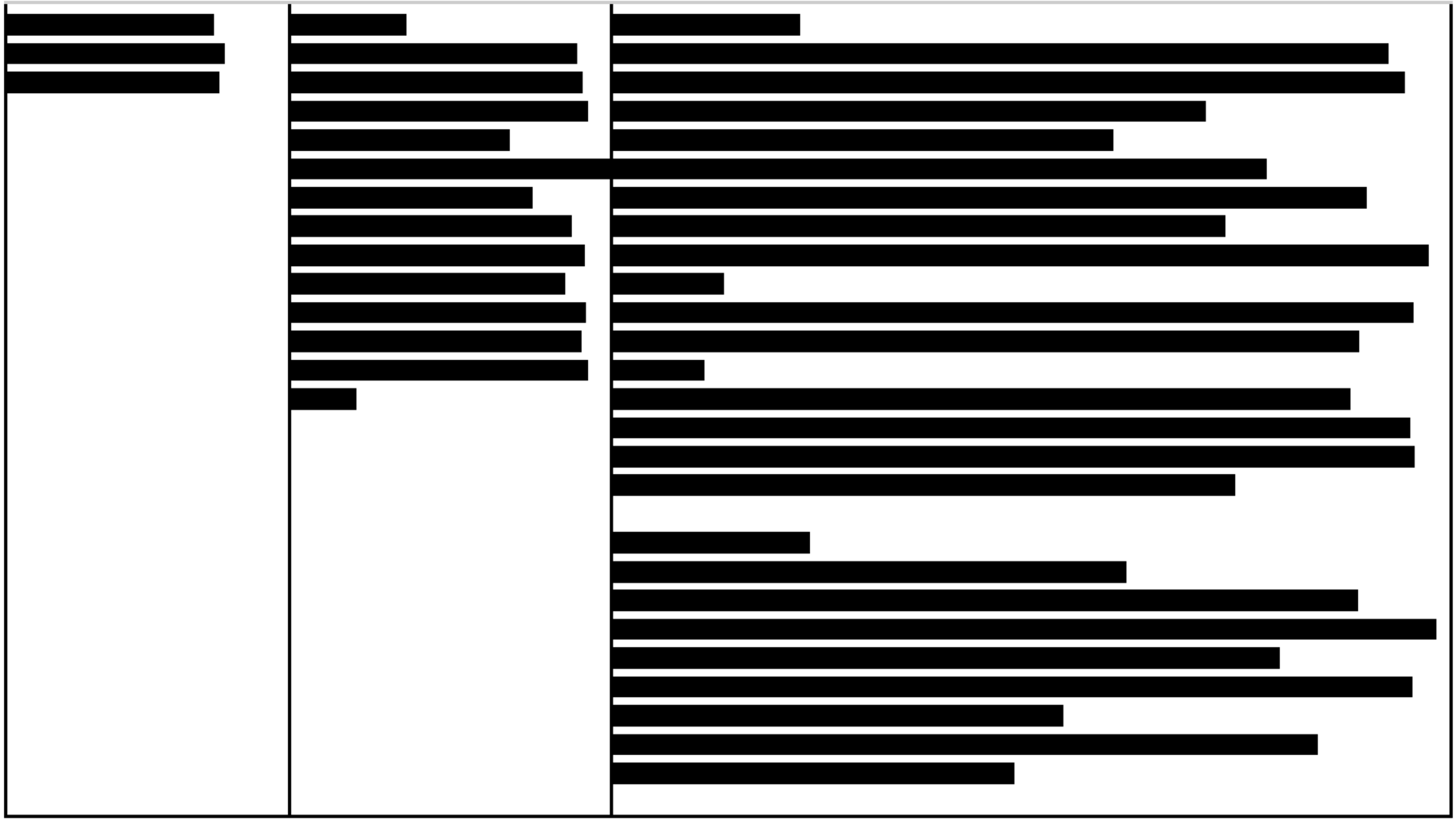
1.5. ANÁLISIS DE RIESGOS

[redacted]	[redacted]		[redacted]	
[redacted]				
[redacted]	[redacted]		[redacted]	





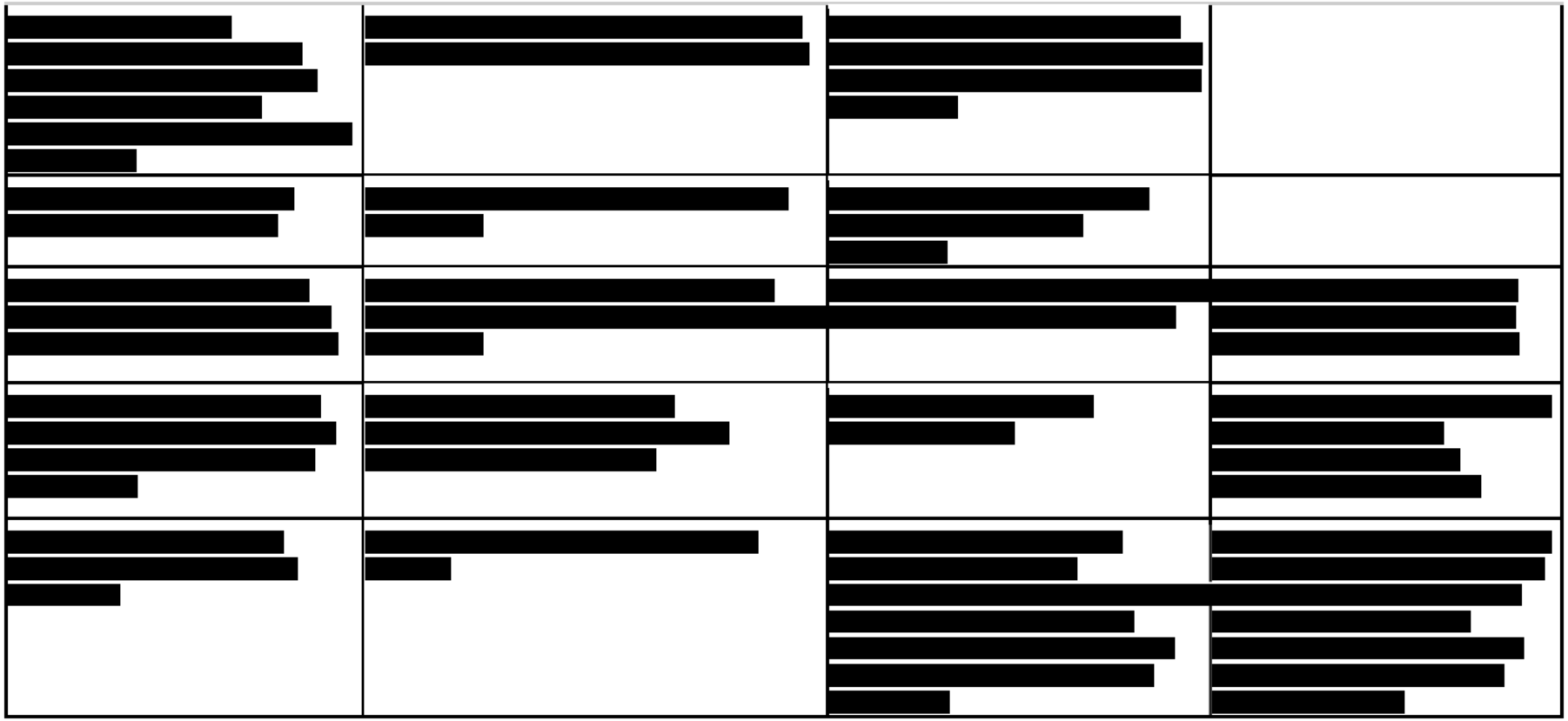
Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
ANÁLISIS DE RIESGOS		
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]



1.6. ANÁLISIS DE BRECHA

Dirección General, DGRU			
Identificador único	IJ1		
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	



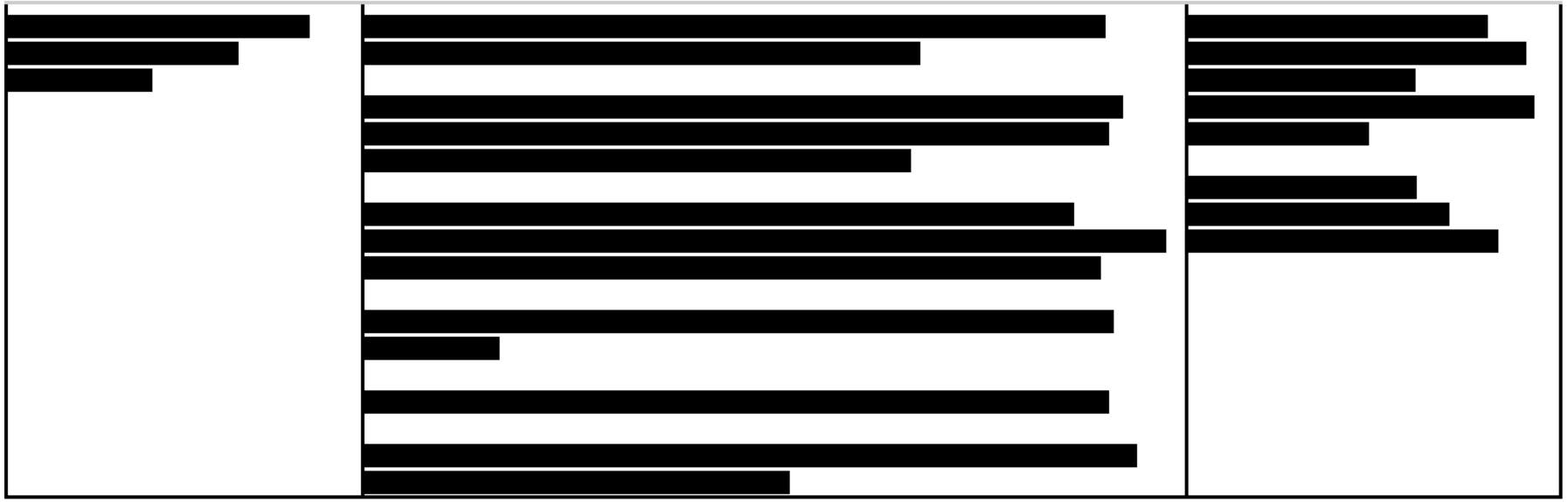
1.7. PLAN DE TRABAJO

Dirección General, DGRU				
Identificador único	IJ1			
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

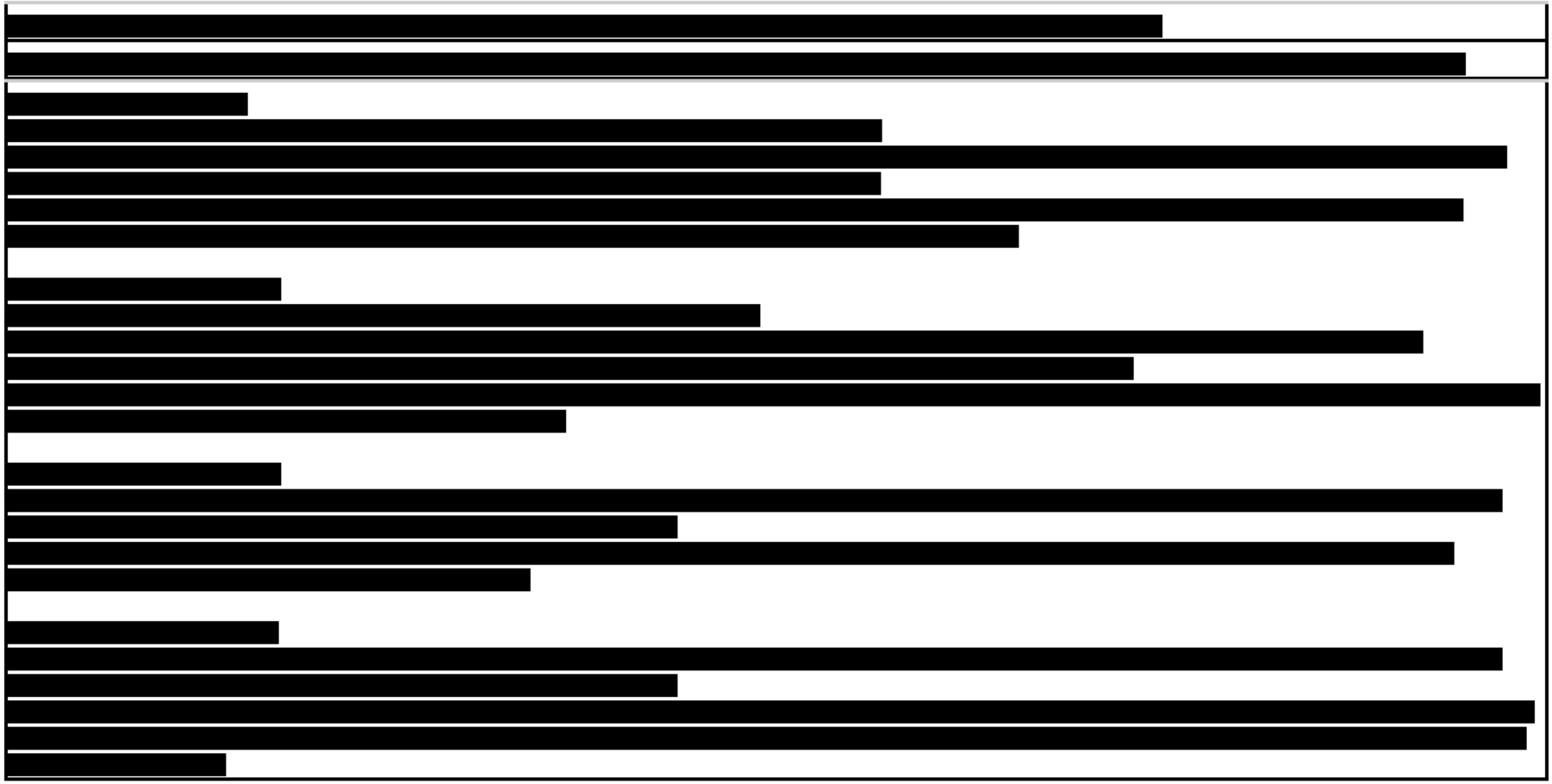
[redacted]	[redacted]		[redacted]	
[redacted]	[redacted]		[redacted]	

1.8. MEDIDAS DE SEGURIDAD

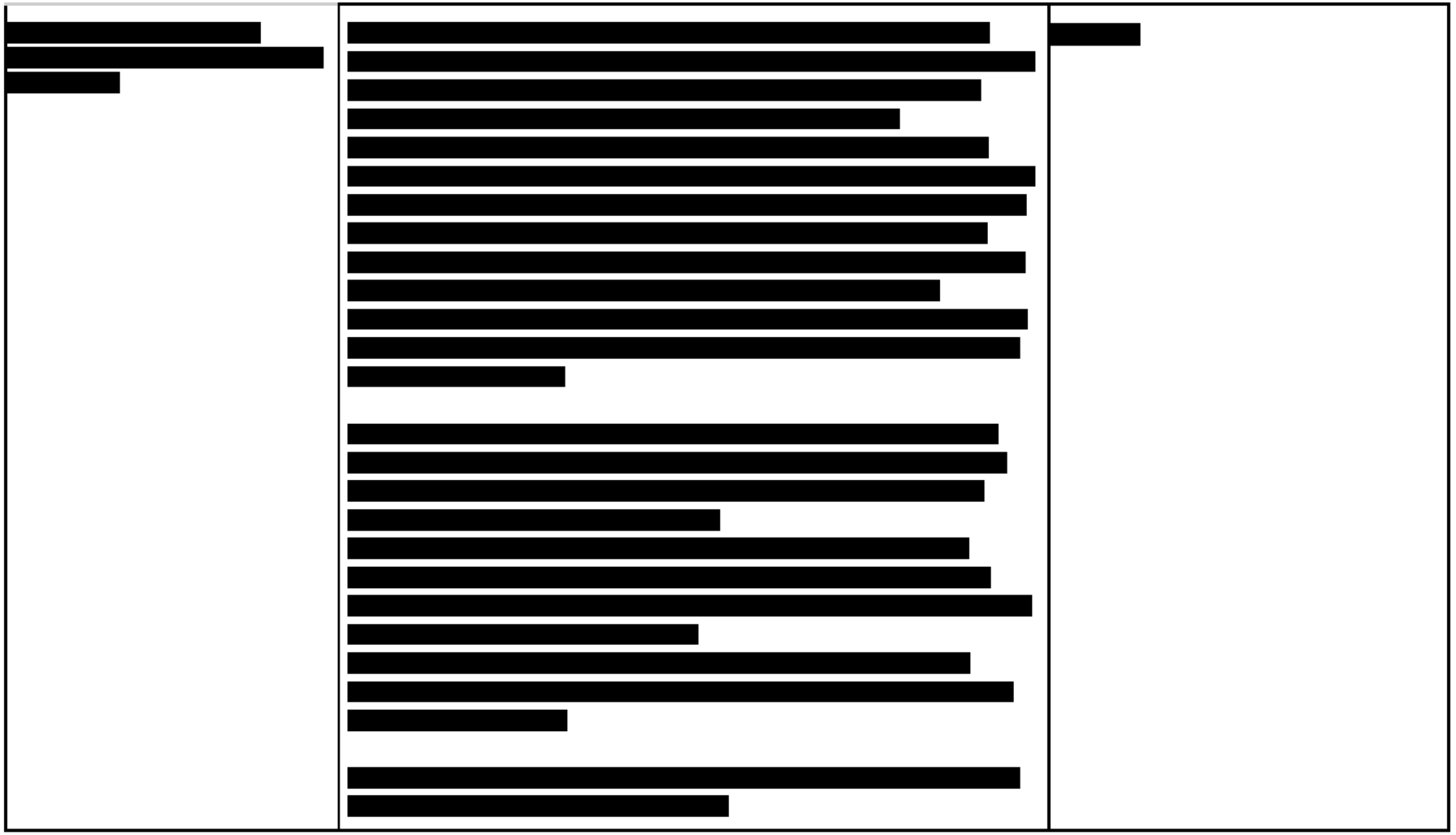
Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]



Dirección General, DGRU	
Identificador único	IJ1
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	



Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]



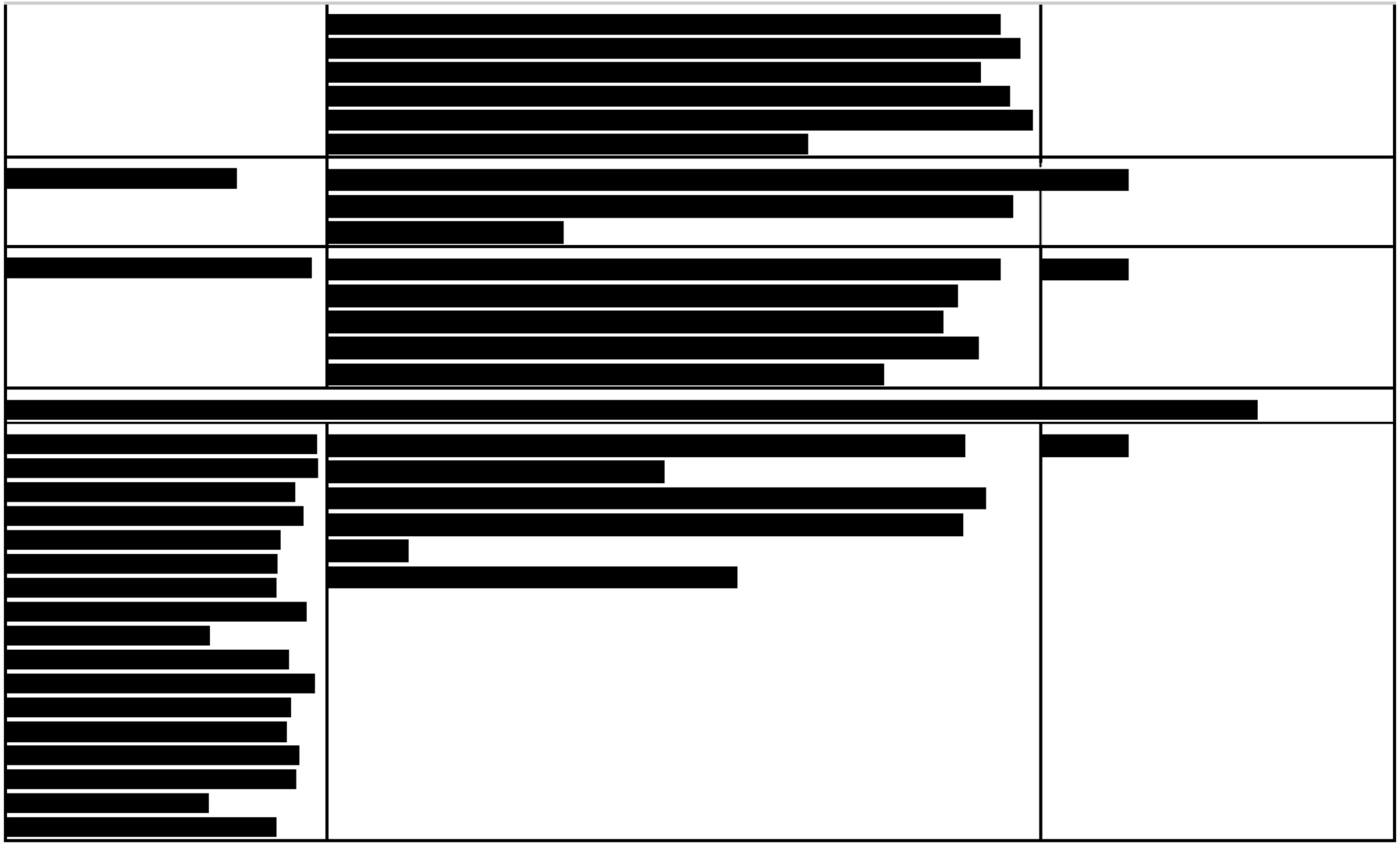
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	[redacted]

		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]		
	[redacted]	

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]



[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]

Dirección General, DGRU	
Identificador único	IJ1
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Dirección General, DGRU	
Identificador único	IJ1
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

[redacted]		

Dirección General, DGRU	
Identificador único	IJ1
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU

IX. PLAN DE CONTINGENCIA

	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

1.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
Medida de seguridad	**Resultado de evaluación**	**Responsable**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Dirección General, DGRU		
Identificador único	IJ1	
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted].

1.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU

Identificador único	IJ1			
Nombre del sistema IJ1	Instrumentos jurídicos de la DGRU			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Dirección General, DGRU				
Identificador único	**IJ1**			
Nombre del sistema IJ1	**Instrumentos jurídicos de la DGRU**			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**

Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales. - Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Procedimientos de borrado seguro de correos electrónicos y de archivos. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones de Desarrollo Tecnológico e Infraestructura, Sistema de Repositorios Universitarios, Colecciones de Datos e Investigación, de Planeación, Gestión y Normatividad y Dirección General. Frecuencia de la actualización una vez al año o antes si se considera necesario.	Alta

Anexo 2. PE1 Apoyo de gestión administrativa del personal

2.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	PE1
Nombre del sistema PE1	Apoyo de gestión administrativa del personal
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, fotografía, idioma o lengua. 1b. Datos laborales: Documentos de reclutamiento y selección, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales. 1c. Datos patrimoniales: información fiscal, ingresos, cuentas bancarias. 1d. Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales: Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia penal, administrativa, con independencia de su etapa de trámite. 1e. Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos.
¿Cómo se obtienen los datos personales?	Físico (X) Digital (X)

¿Para qué se usan?	Los datos señalados en los incisos 1a, 1b, 1c, 1e se usan para el apoyo en la gestión del proceso de contratación del personal que realiza la unidad administrativa de la Secretaría de Desarrollo Institucional. Los datos señalados en el inciso 1d se utilizan cuando existe un proceso de gestión asociado al robo de bienes de la dependencia.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal ( )	Gobierno Estatal ( ) Gobierno Municipal ( ) Personas físicas (X) Personas morales ( ) Áreas Universitarias (X) Para la gestión del proceso de contratación del personal. Para el proceso de gestión asociado al robo de bienes de la dependencia.

¿Dónde se alojan?	[redacted]
¿Cuánto tiempo se da tratamiento?	1) Los datos señalados en los incisos 1a, 1b, 1c, 1e desde que inicia el proceso de gestión de contratación de personal hasta que el personal queda contratado (aproximadamente un mes). 2) Los datos señalados en el inciso 1d se resguardan desde que el personal es contratado hasta el término de su contratación (lo que dure el contrato).
Responsable	
Nombre:	Tila María Pérez Ortiz
Cargo:	Directora General de Repositorios Universitarios

Funciones:	Revisar, y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez revisada la información del proceso de contratación se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Co-Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad
Funciones:	Recabar, revisar, y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez recabada y revisada la información del proceso de contratación se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación
Funciones:	Recabar, revisar, y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez recabada y revisada la información del proceso de contratación se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.

Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Informática
Funciones:	Recabar, revisar, y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez recabada y revisada la información del proceso de contratación se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Rubén Ignacio Sáenz González
Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Recabar, revisar, y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez recabada y revisada la información del proceso de contratación se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Areli Plancarte Salas

Cargo:	Asistente Ejecutivo
Funciones:	Recabar, revisar, registrar, organizar, comunicar, almacenar y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez recabada, revisada, registrada y organizada, comunica la información a la Secretaría de Desarrollo Institucional para el proceso de contratación y si procede, almacena la información en un espacio de encriptado de la DGRU; en caso contrario la información se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Encargado	
Nombre:	José Antonio Contreras Morales
Cargo:	Encargado de gestión administrativa
Funciones:	Recabar, revisar, registrar, organizar, comunicar, almacenar y suprimir la información relativa a la gestión del personal.
Obligaciones:	Una vez recabada, revisada, registrada y organizada, comunica la información a la Secretaría de Desarrollo Institucional para el proceso de contratación y si procede, almacena la información en un espacio de encriptado de la DGRU; en caso contrario la información se suprime de forma segura. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Encargados	

Nombre:	Alejandro Chávez Méndez
Cargo:	No Aplica
Funciones:	Resguardar de manera segura los datos personales contenidos en los documentos físicos relativos con las actas de robo de bienes de la DGRU
Obligaciones:	Archivar el documento físico conforme al procedimiento interno de la DGRU. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General

2.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	PE1
Nombre del sistema PE1	Apoyo de gestión administrativa del personal
Tipo de soporte:	[redacted]
Descripción:	[redacted]

Características del lugar donde se resguardan los soportes:	[redacted]

[redacted]

2.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Documentos relacionados con la contratación del personal y gestión administrativa	Es importante para realizar evaluación de candidatos; cubrir requerimientos del proceso de contratación del personal; seguimiento a procesos administrativos asociados al robo de bienes de la dependencia.	Documentos con información personal requeridos para la evaluación y contratación de candidatos. Actas o documentos probatorios con información personal relacionados al robo de bienes de la dependencia.
Dueño		
¿A quién pertenece el activo de información?		
Responsable de Gestión administrativa del personal		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		

(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	La información recabada para la contratación de personal, únicamente puede ser consultada por las personas asignadas a este proceso. En cuanto a actas y documentos probatorios, sólo el personal involucrado en los procesos administrativos asociados podrá tener acceso.
(X) Integridad	Solo personal autorizado puede modificar este activo de información de la siguiente manera:	Los documentos para el proceso de contratación son eliminados de forma segura en cuanto se envían a la SDI. Actas y documentos probatorios no deben ser alterados.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera:	La versión digital y física de los documentos para la contratación del personal, está disponible para el personal asignado, exclusivamente durante el proceso de contratación. La versión digital y física de la documentación probatoria del robo de bienes de la DGRU está disponible para consulta por el personal autorizado por la DGRU.
( ) Otro		
Requisitos de seguridad más importante		

¿Cuál es el requisito de seguridad más importante para este activo?			
(X) Confidencialidad	**( ) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	

INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	
[redacted]	

2.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Apoyo de gestión administrativa del personal
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]			
[redacted]			
[redacted]			
[redacted]			

CONTENEDORES FÍSICOS

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]

[redacted]

[redacted]

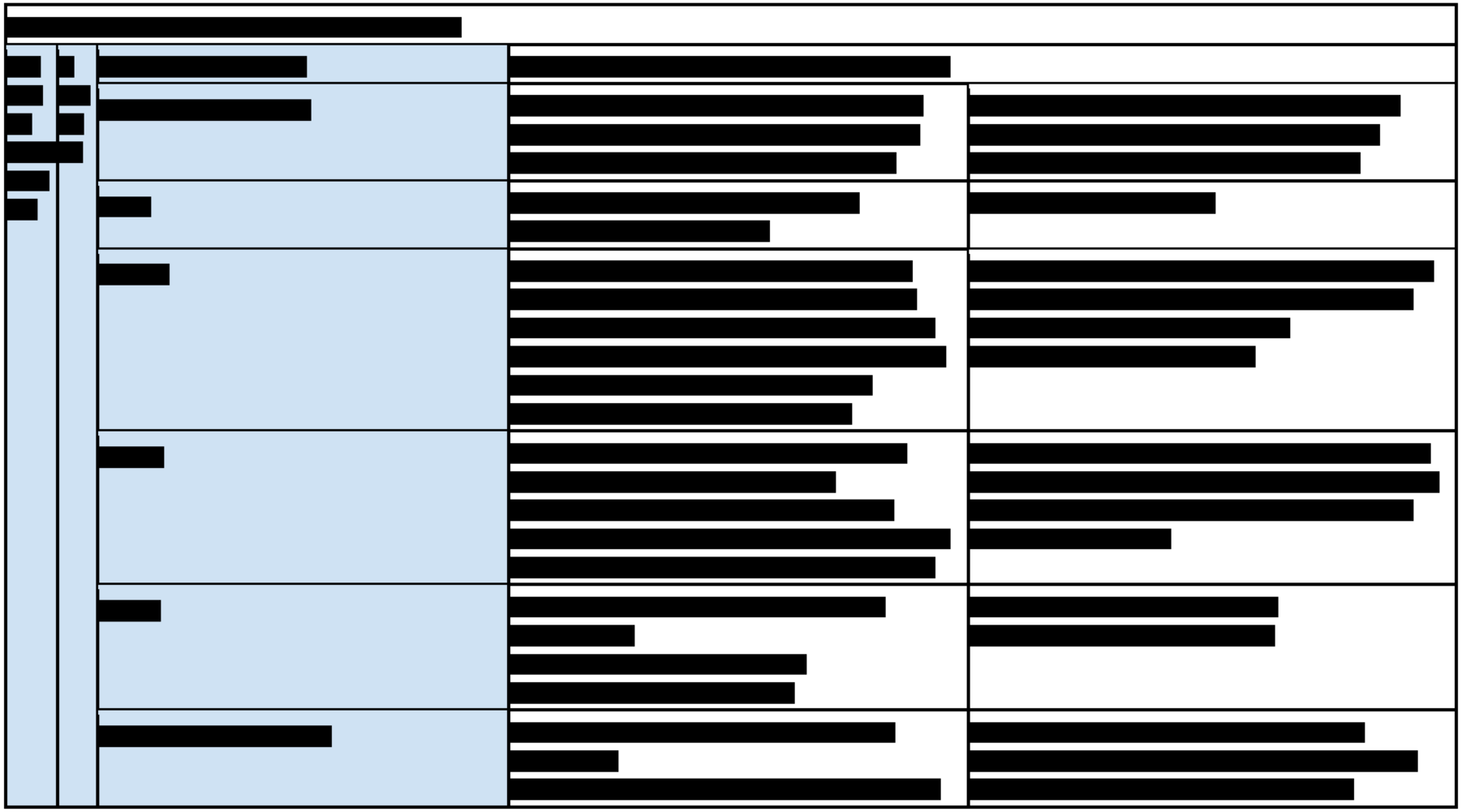
RECURSOS HUMANOS

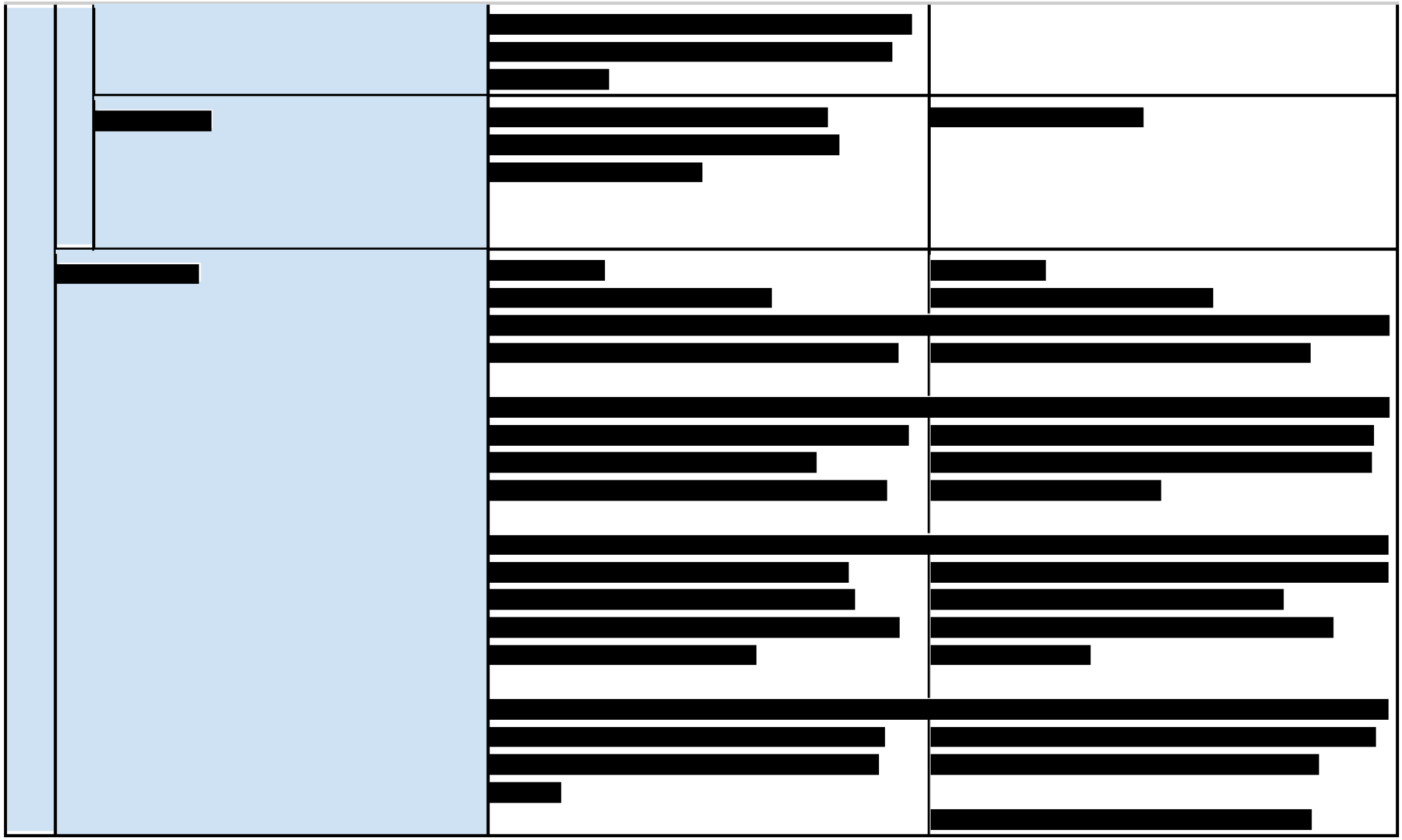
[redacted]

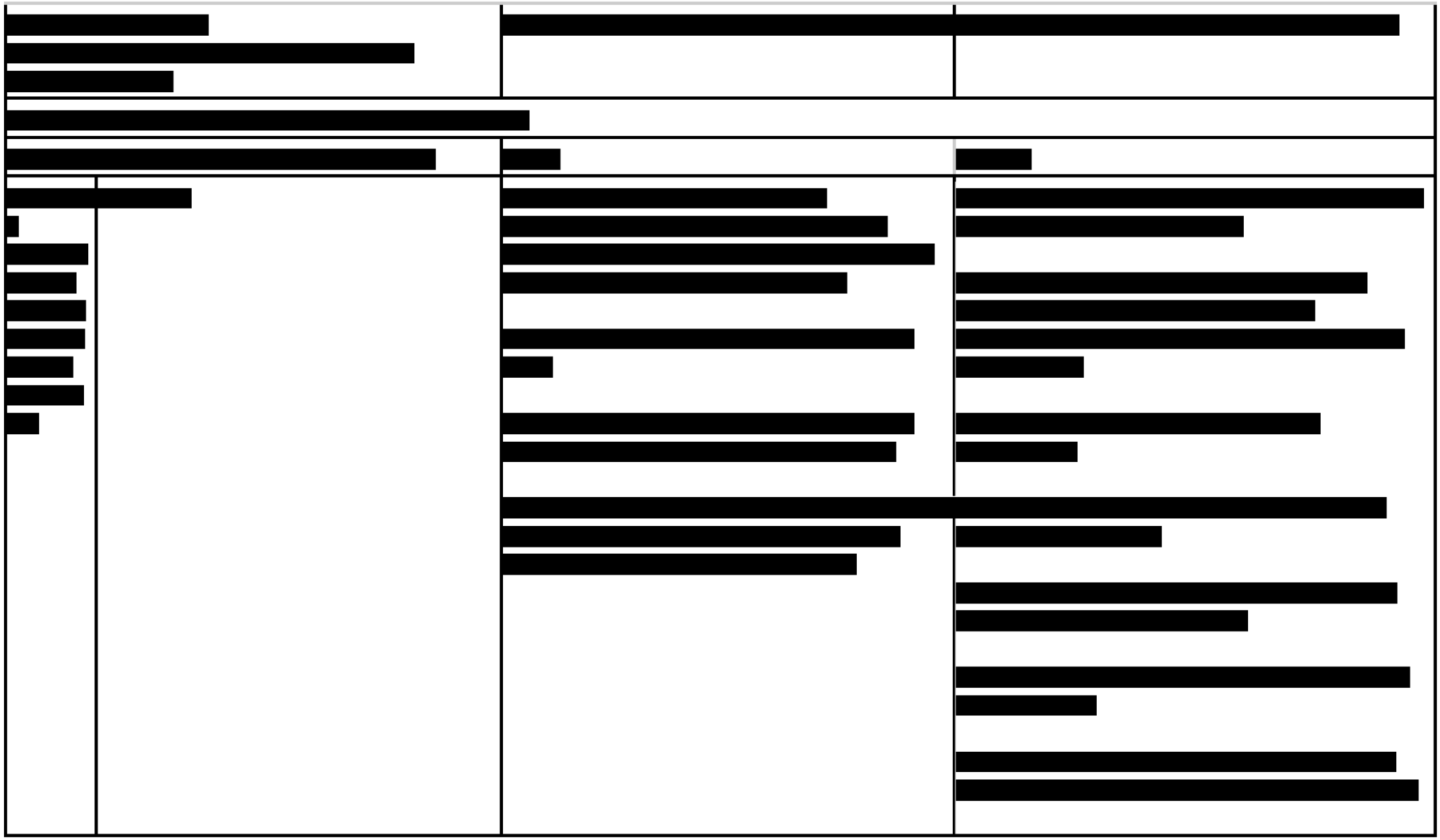
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

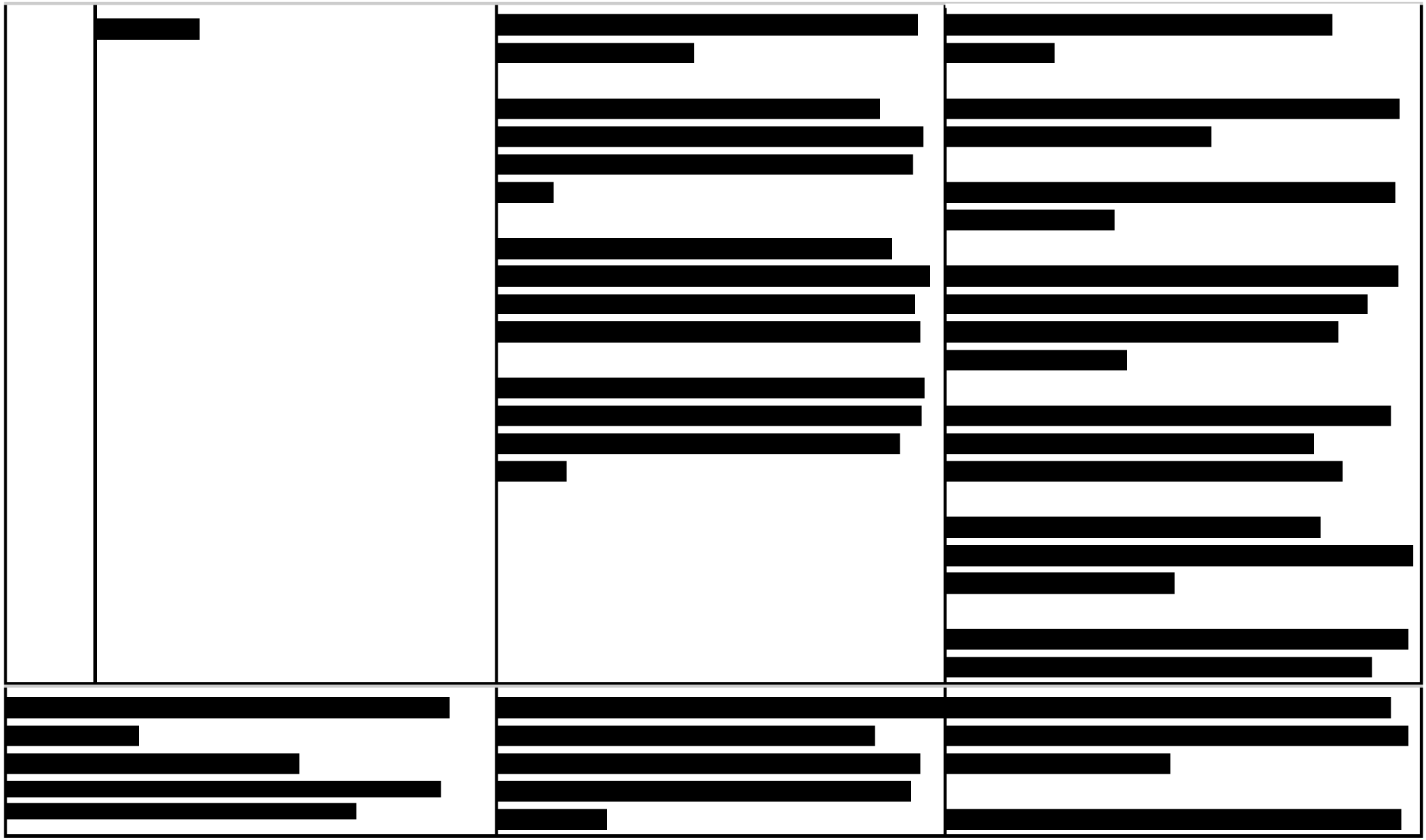
2.5. ANÁLISIS DE RIESGOS

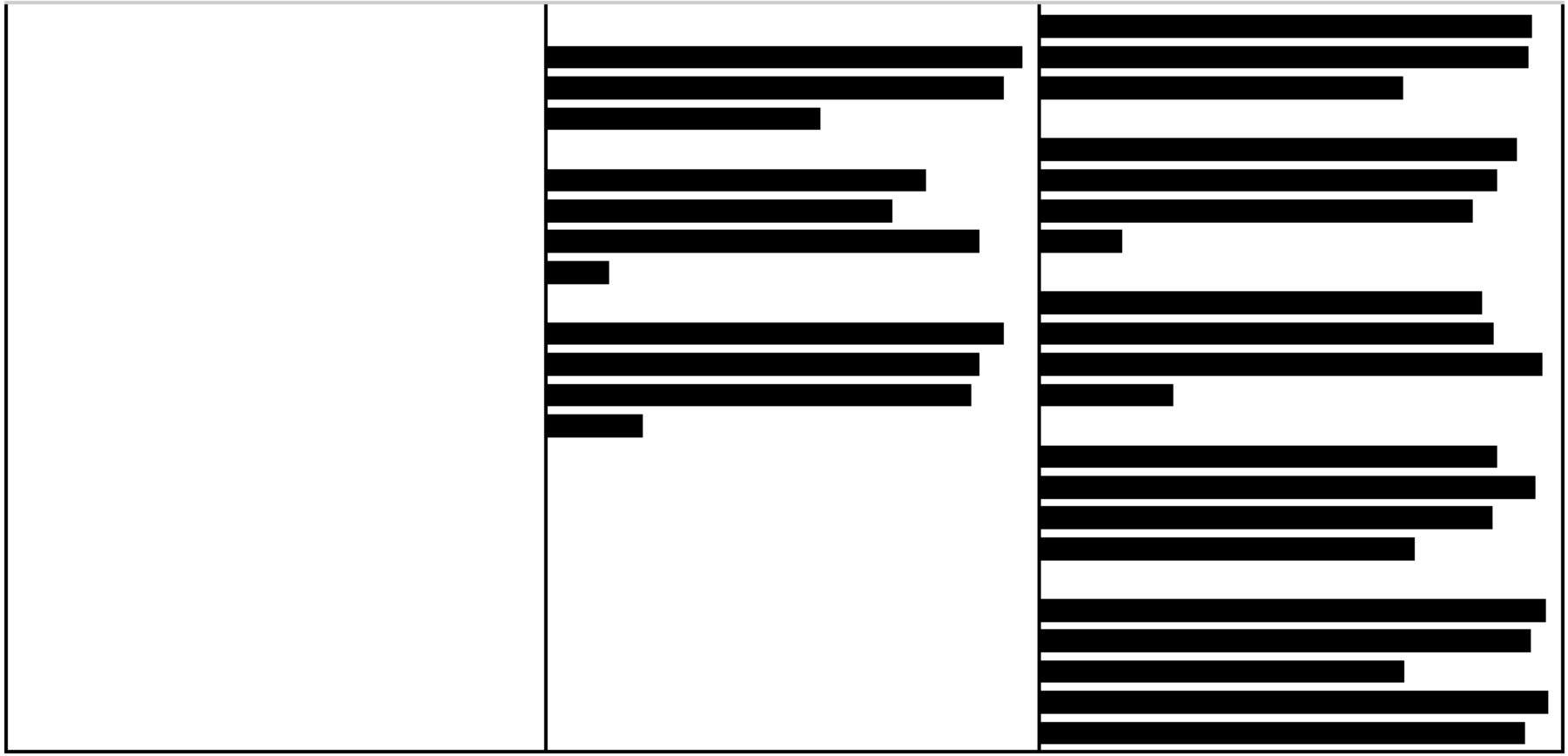




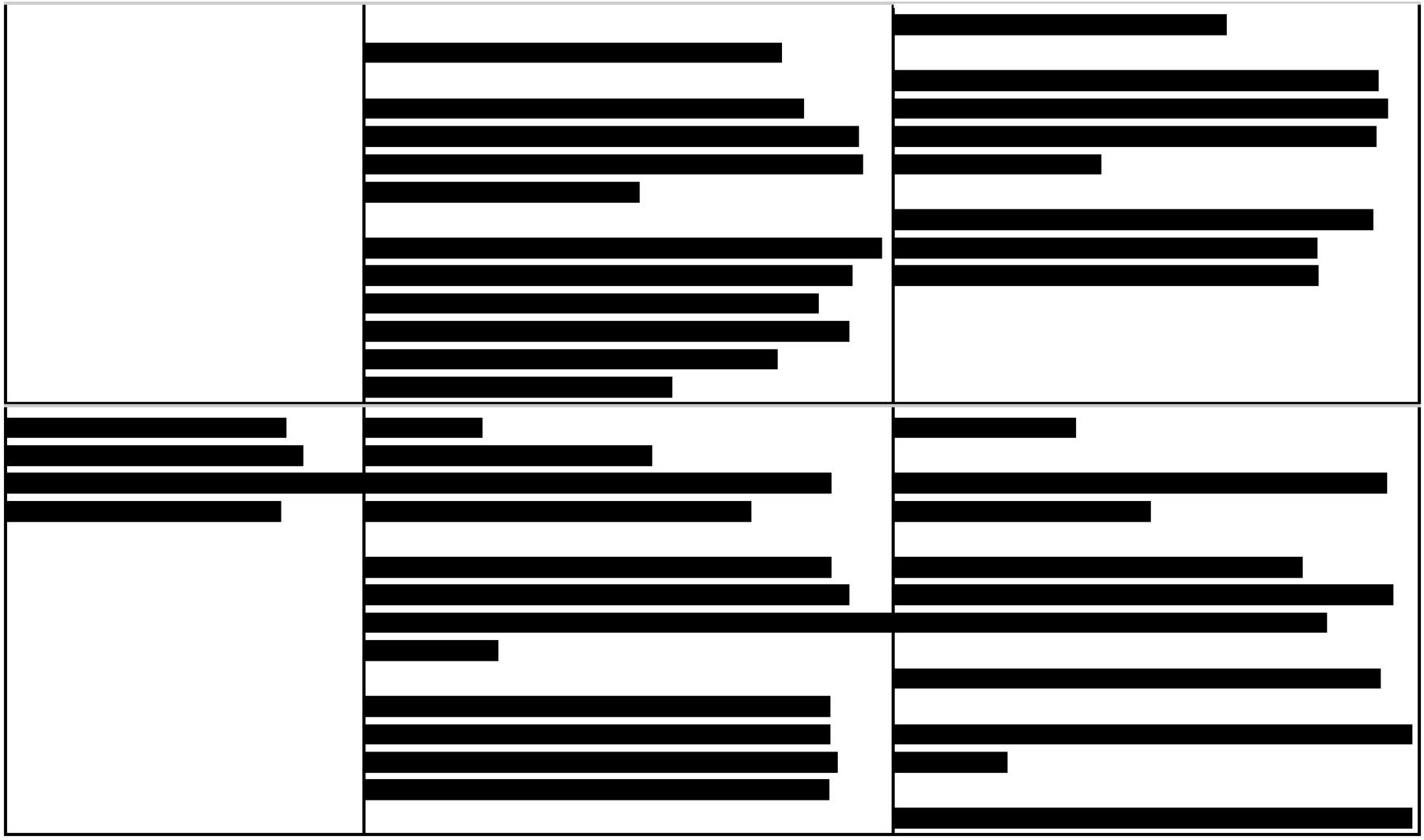


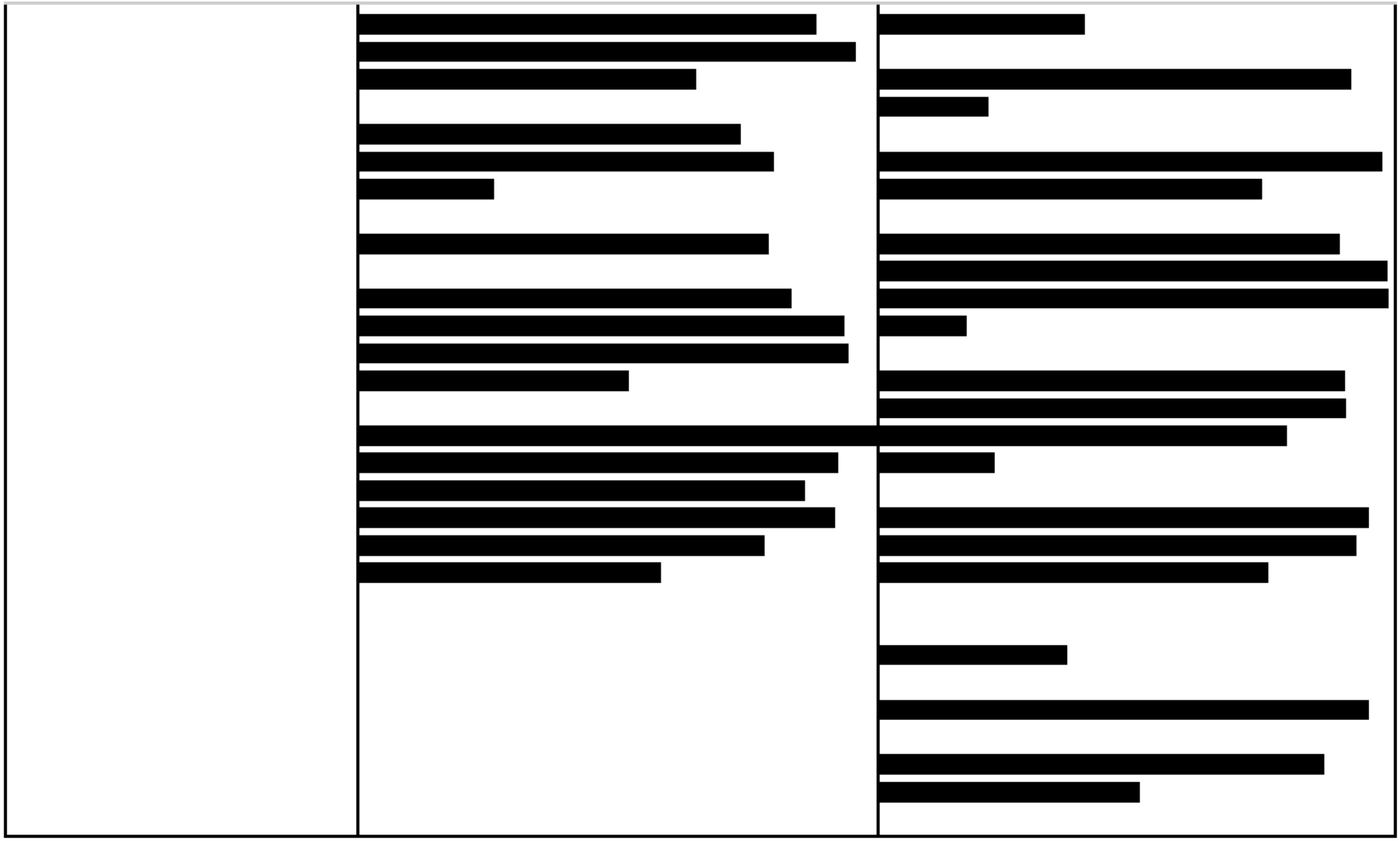
			[redacted]





Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
ANÁLISIS DE RIESGOS		
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]





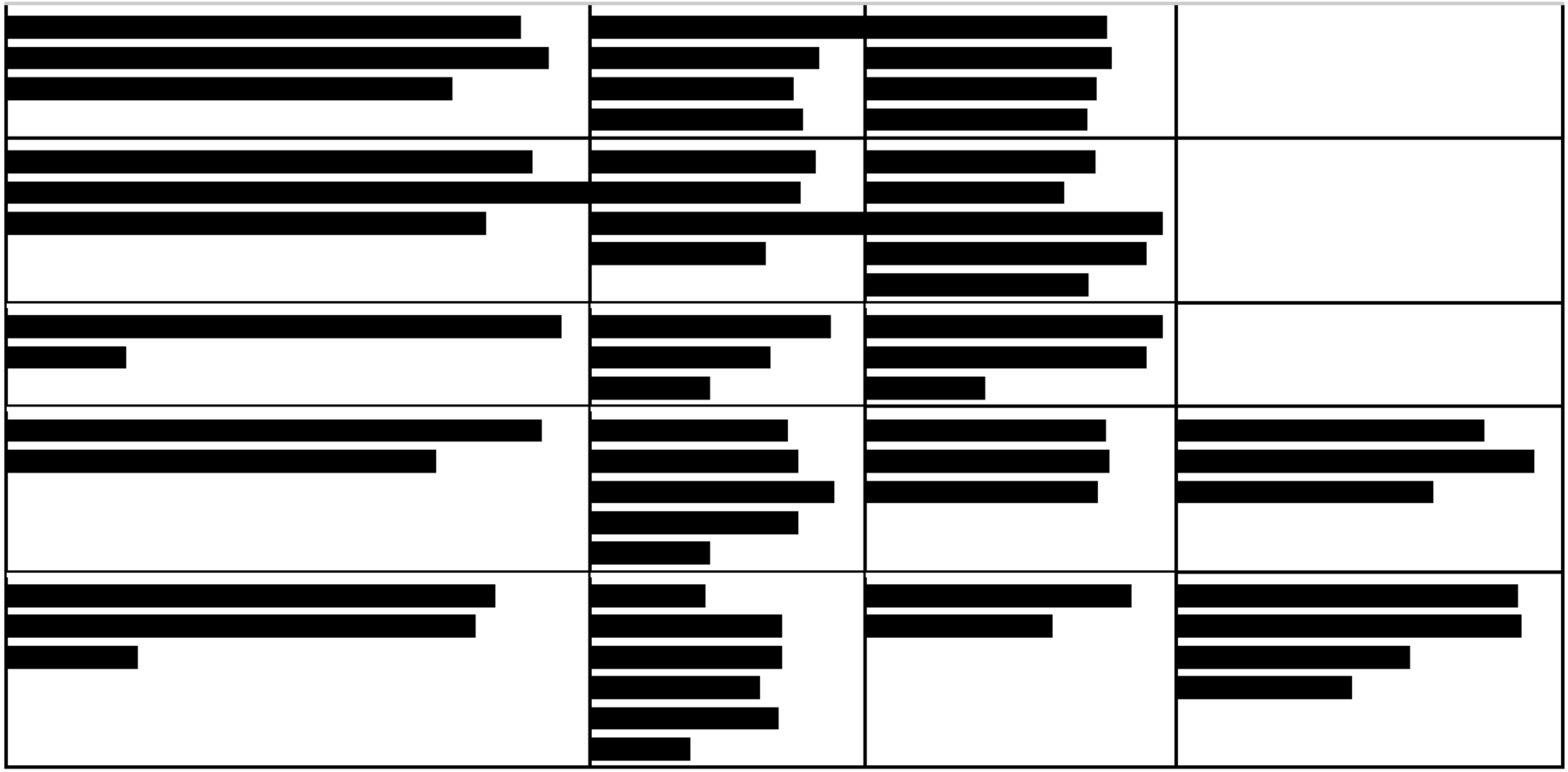
		[redacted]

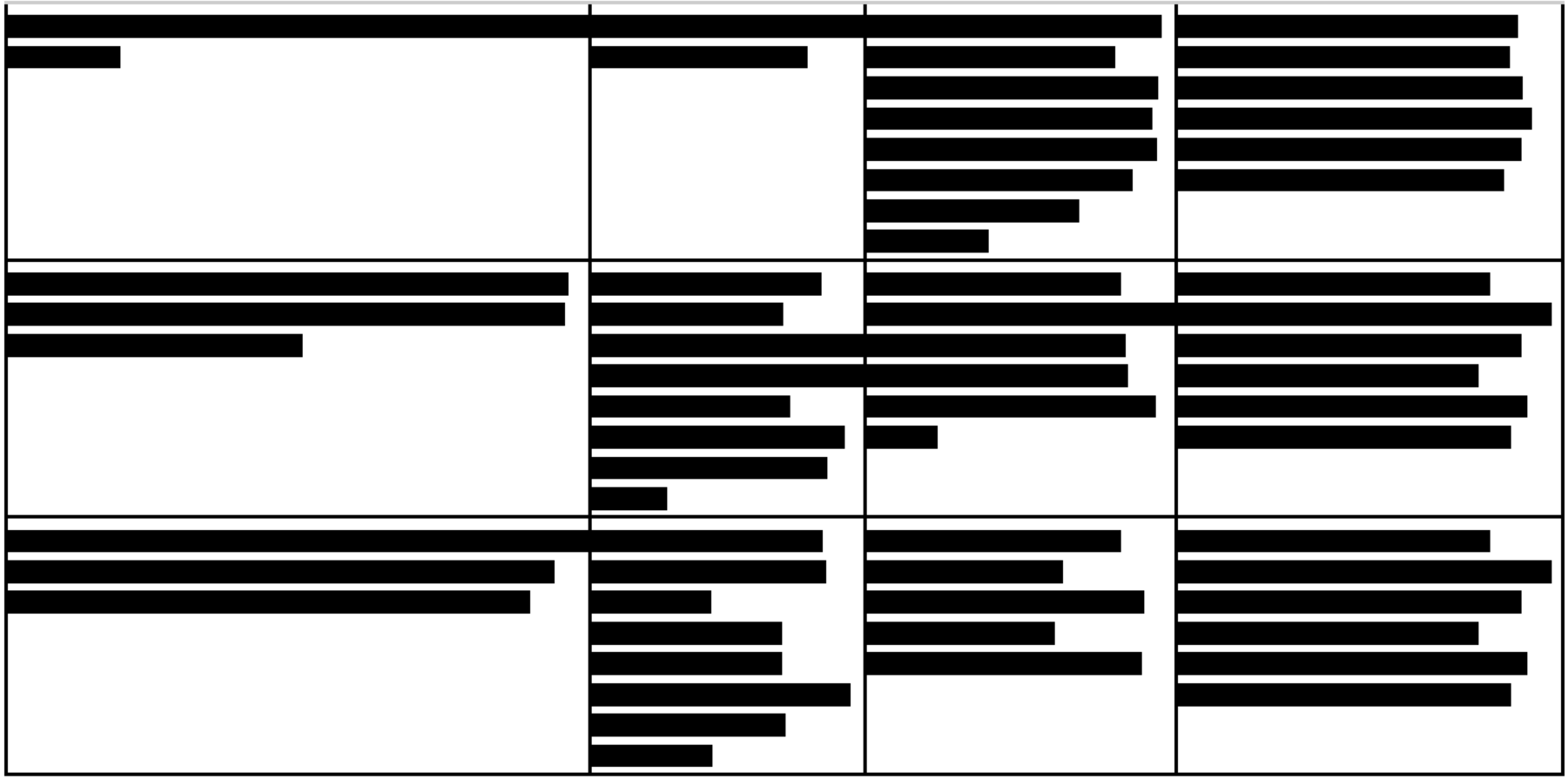
2.6. ANÁLISIS DE BRECHA

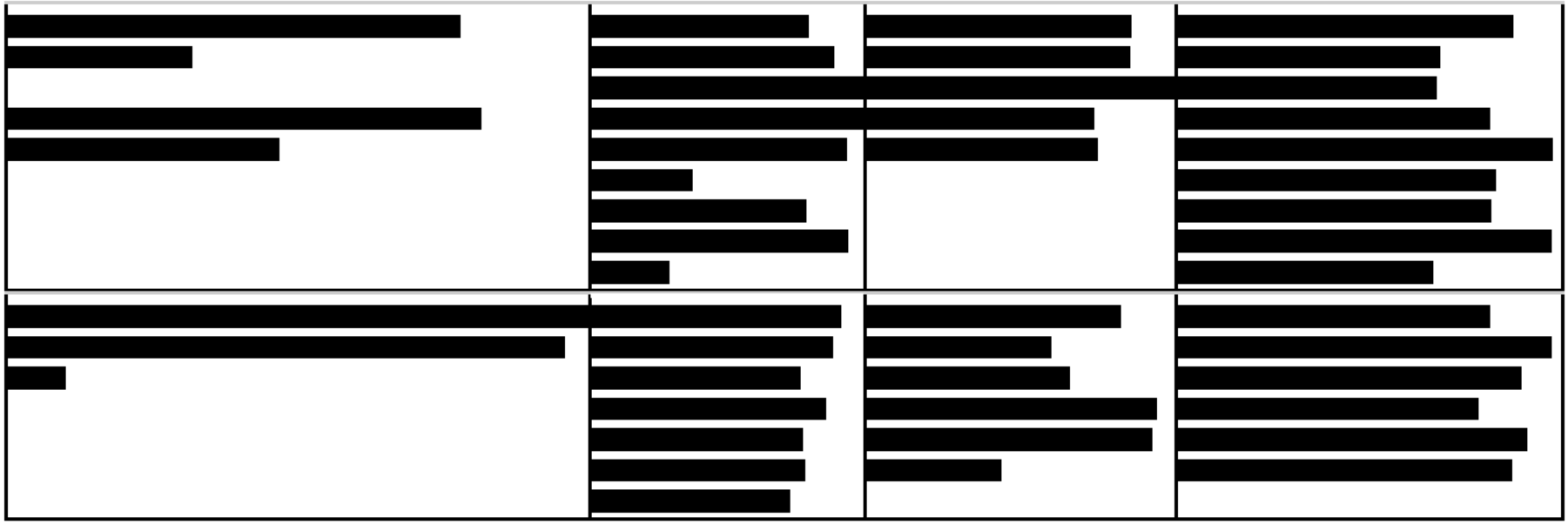
Dirección General, DGRU			
Identificador único	PE1		
Nombre del sistema PE1	Apoyo de gestión administrativa del personal		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**

[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		







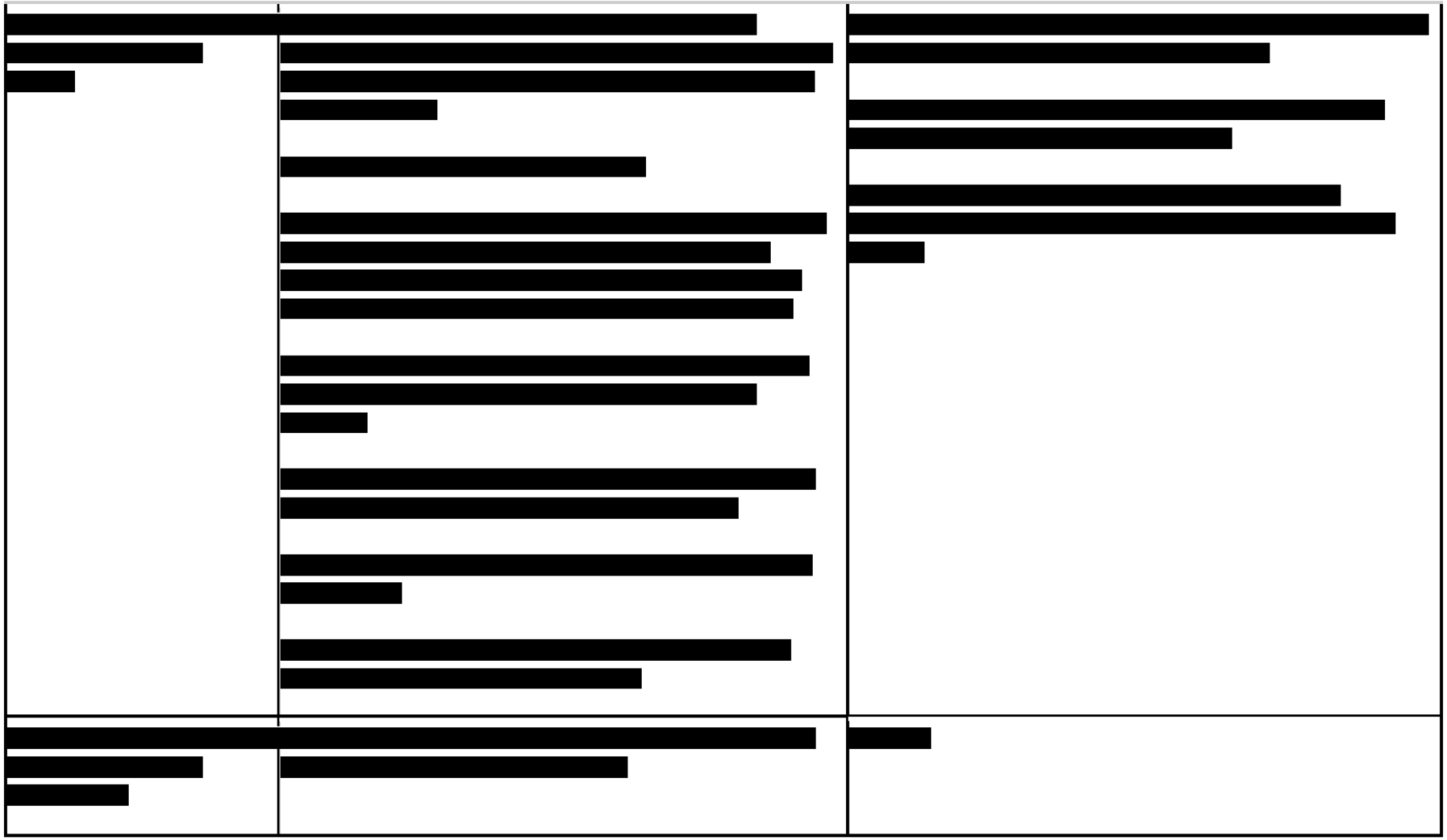
2.7. PLAN DE TRABAJO

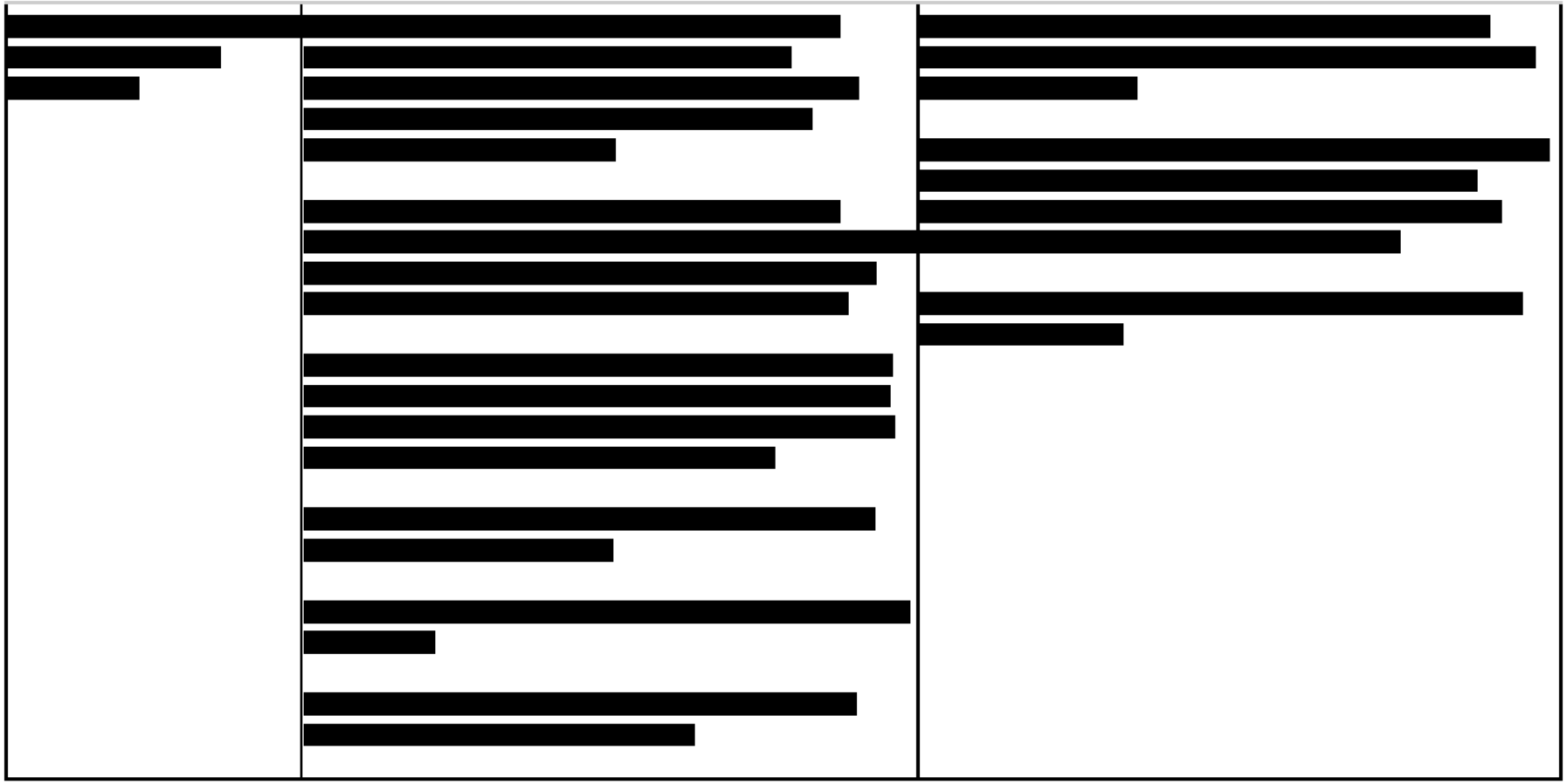
Dirección General, DGRU				
Identificador único	PE1			
Nombre del sistema PE1	Apoyo de gestión administrativa del personal			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**

[redacted]			

2.8. MEDIDAS DE SEGURIDAD

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**



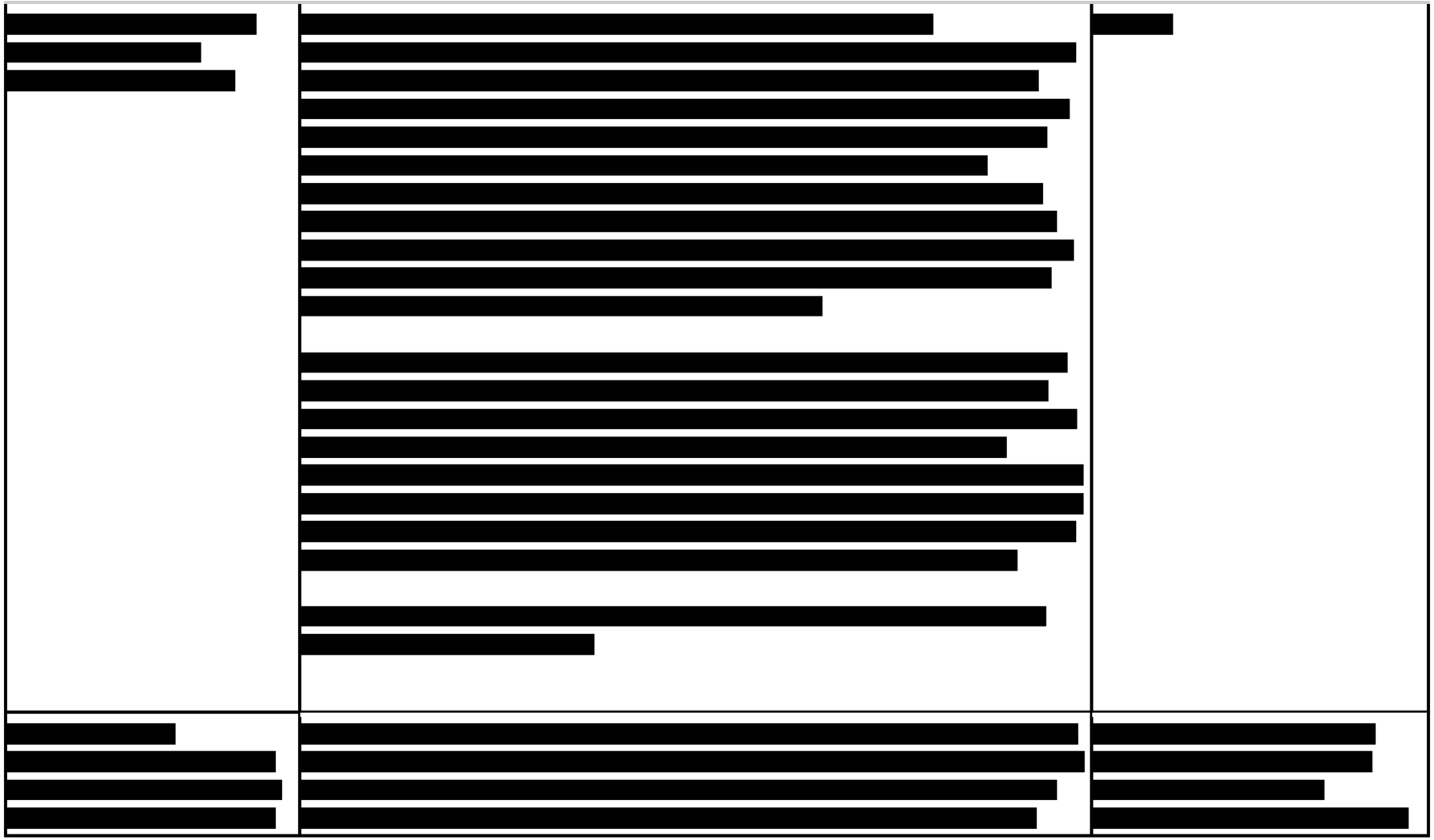


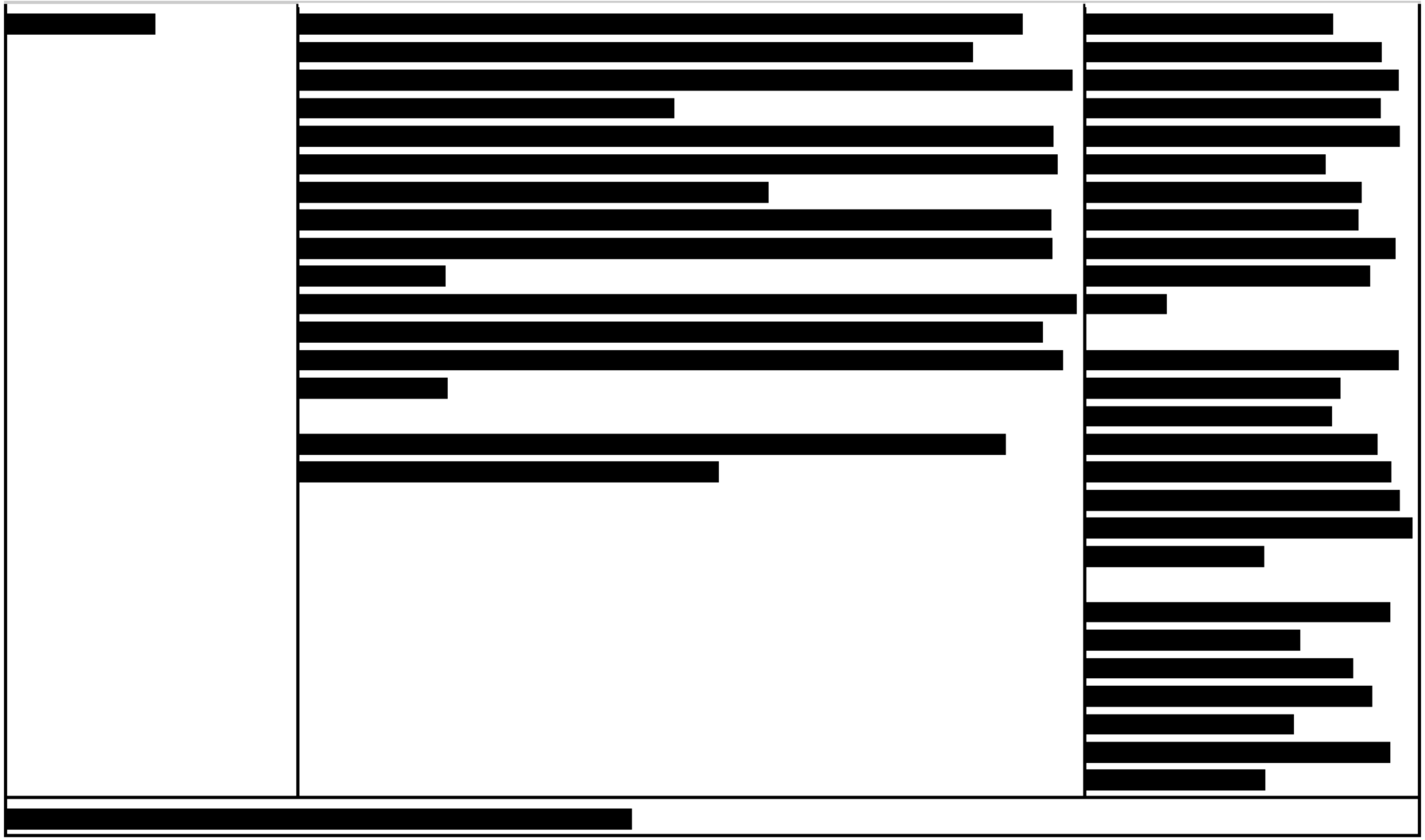
Dirección General, DGRU	
Identificador único	PE1
Nombre del sistema PE1	Apoyo de gestión administrativa del personal
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	
[redacted]	
[redacted]	

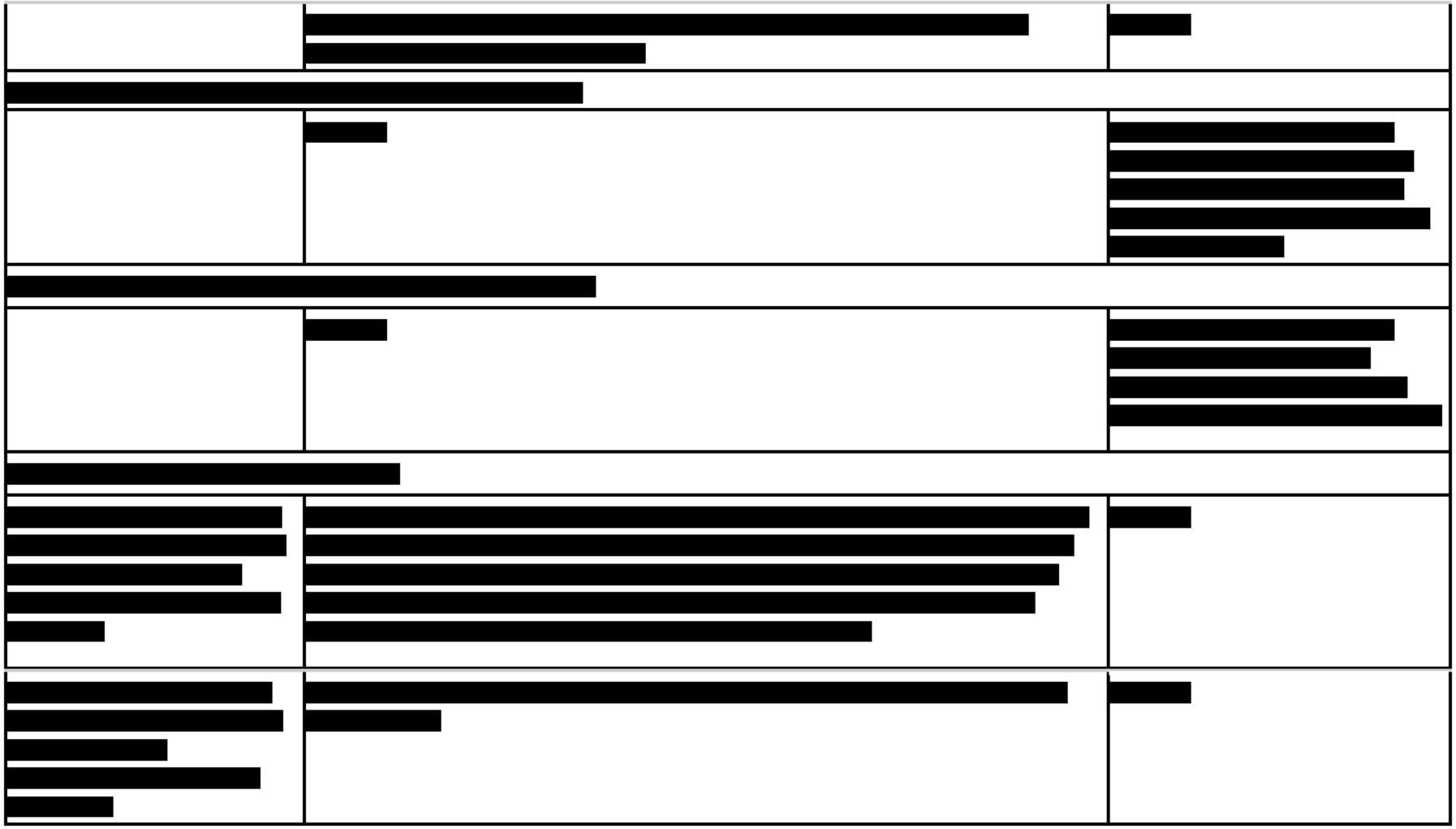
[redacted]

Dirección General, DGRU	
Identificador único	PE1
Nombre del sistema PE1	Apoyo de gestión administrativa del personal

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		



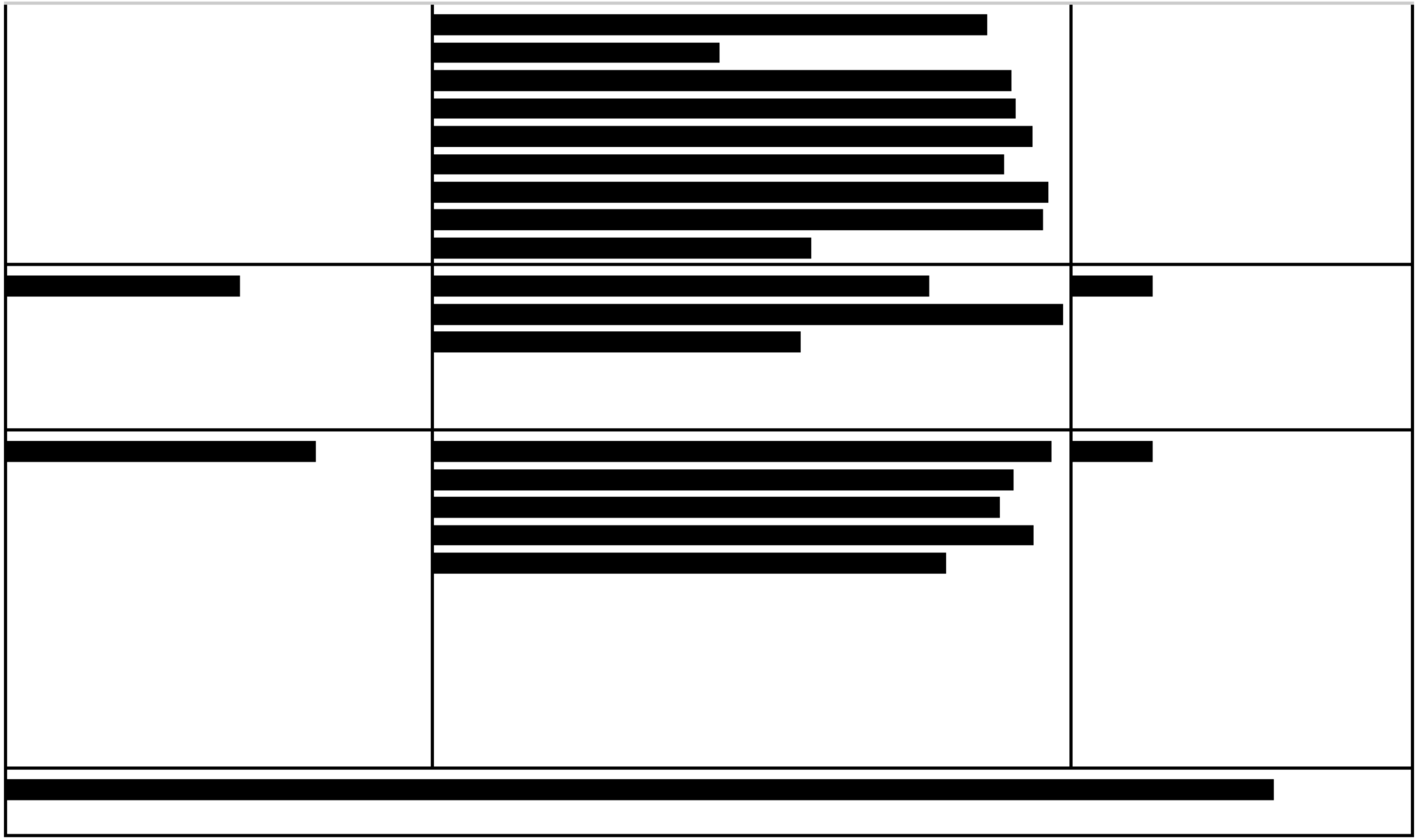


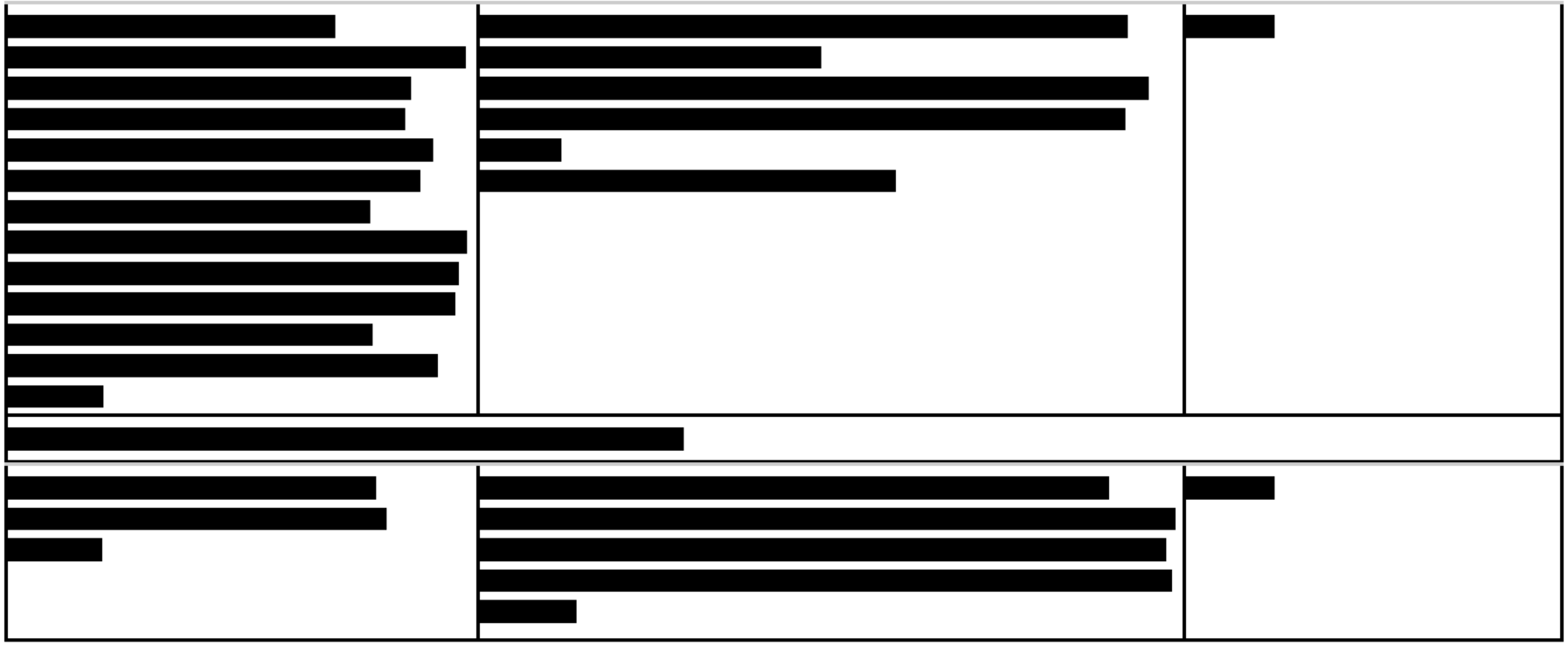


Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]		
	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]

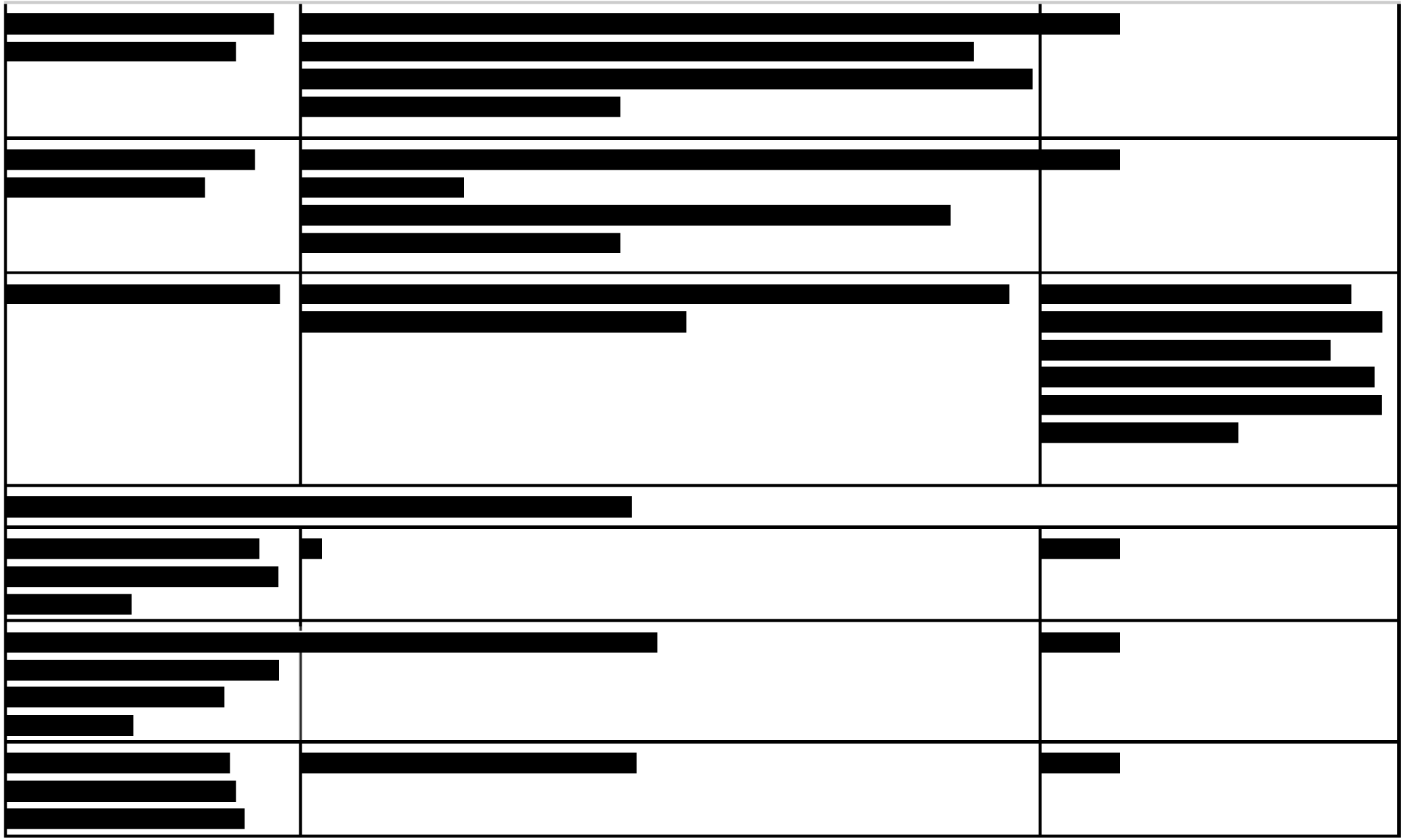


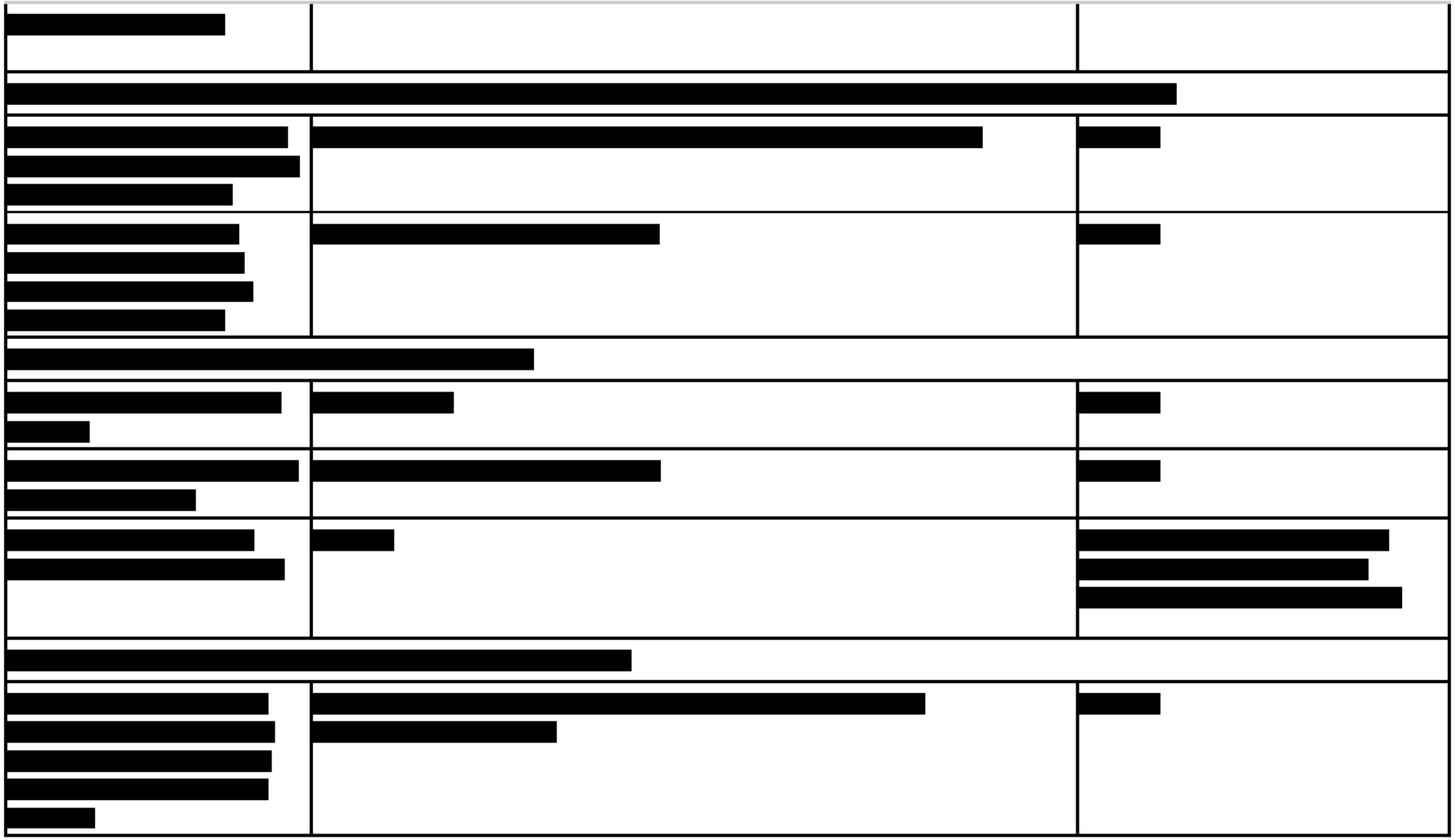


Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**

[redacted]		[redacted]

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]

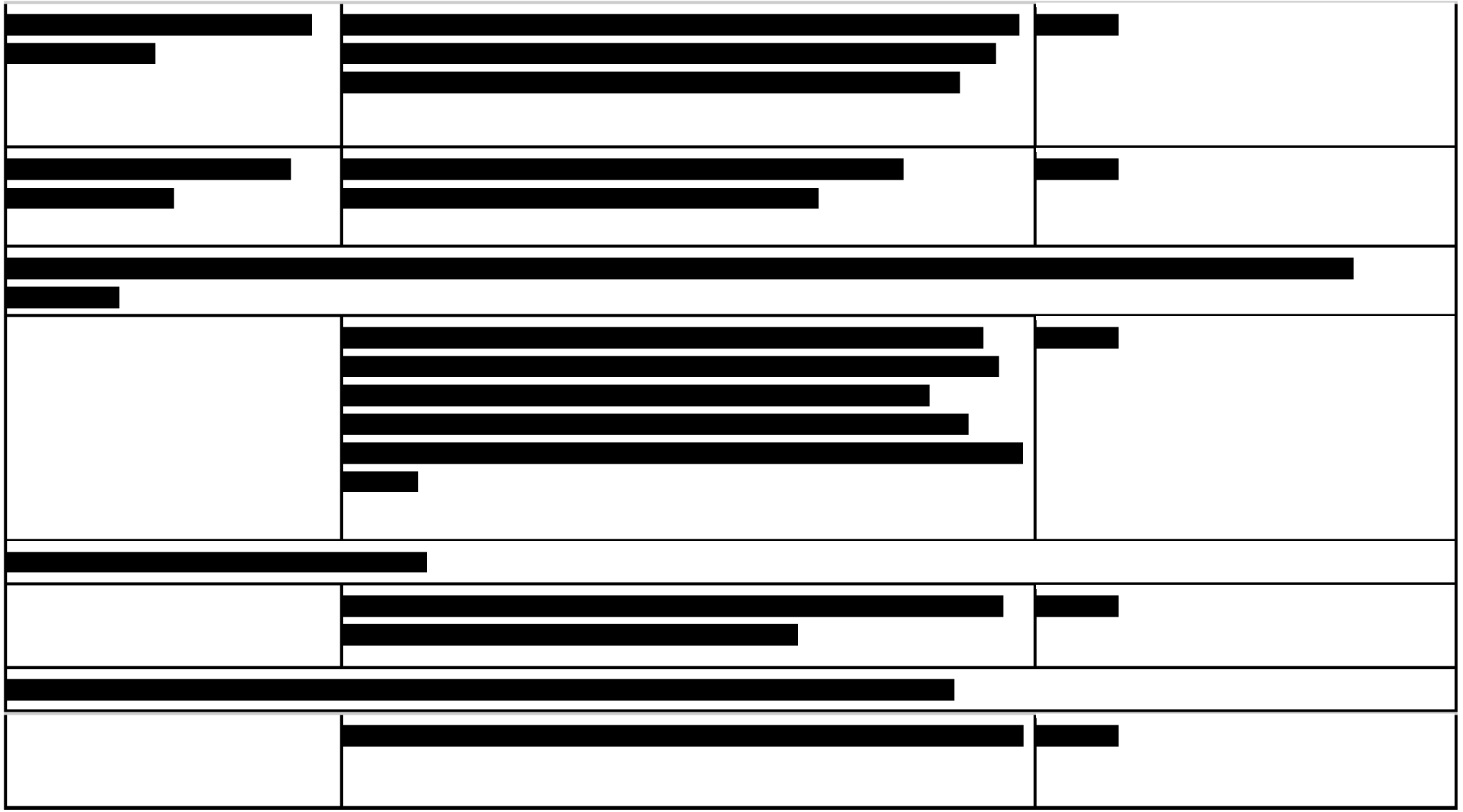




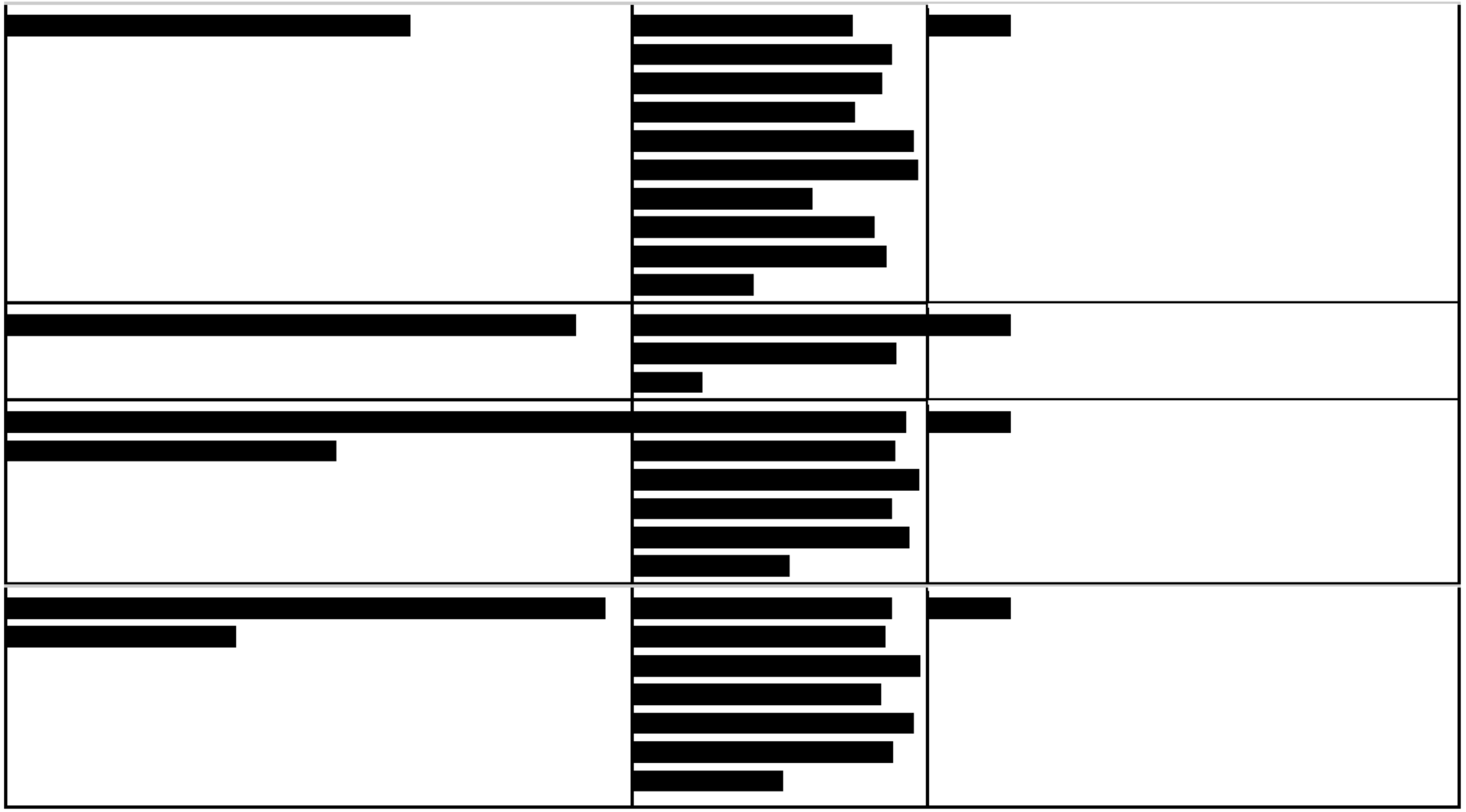
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Dirección General, DGRU	
Identificador único	PE1
Nombre del sistema PE1	Apoyo de gestión administrativa del personal
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	

	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]



Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		



2.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
Medida de seguridad	**Procedimiento**	**Responsable**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Dirección General, DGRU		
Identificador único	PE1	
Nombre del sistema PE1	Apoyo de gestión administrativa del personal	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

2.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU				
Identificador único	PE1			
Nombre del sistema PE1	Apoyo de gestión administrativa del personal			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Dirección General, DGRU				
Identificador único	PE1			
Nombre del sistema PE1	Apoyo de gestión administrativa del personal			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales, - Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Procedimientos de borrado seguro de correos electrónicos y de archivos; - Uso adecuado de sesiones en la plataforma y en los equipos del personal.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones de Desarrollo Tecnológico e Infraestructura, Sistema de Repositorios Universitarios, Colecciones de Datos e Investigación, coordinación de Planeación, Gestión y Normatividad y Dirección General. Frecuencia de la actualización una vez al año o antes si se considera necesario.	Alta

Anexo 3. PE2 Gestión sanitaria y emergencias

3.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
Datos personales (sensible o no) contenidos en el sistema:	1. Datos personales en general: 1a. Datos de identificación: nombre, domicilio, teléfono particular, teléfono celular, fecha de nacimiento, edad, nombres y número telefónico de personas para contacto en caso de emergencia. 1b: Datos laborales: número de trabajador y cargo. 2. Datos personales sensibles: estado de salud (alergias, enfermedades, medicamentos).	
¿Cómo se obtienen los datos personales?	Físico (X) Digital (X)	
¿Para qué se usan?	Los datos se usan para atender la comunicación necesaria en caso de una emergencia y para registrar los datos de seguimiento en la plataforma informática "Bitácora del responsable sanitario" conforme a las disposiciones del Comité de Seguimiento COVID-19.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?

	Gobierno Federal ( )	Gobierno Estatal ( ) Gobierno Municipal ( ) Personas físicas (X) Personas morales ( ) Áreas Universitarias (X) Los datos de las fichas de emergencia se comparten para establecer comunicación y brindar atención médica necesaria en caso de una emergencia. Los datos para el seguimiento COVID-19 se recaban mediante videoconferencia entre el titular de los datos personales y el responsable sanitario quien registra la información necesaria en la plataforma informática y no se conserva copia alguna.
¿Dónde se alojan?	[redacted]	
¿Cuánto tiempo se da tratamiento?	Desde que el personal es contratado hasta el término de su contratación (lo que dure el contrato).	

Responsable	
Nombre:	Areli Plancarte Salas
Cargo:	Asistente Ejecutivo
Funciones:	Recabar, almacenar y suprimir la información relativa a la gestión del personal. En caso de emergencia, disponer de la maleta de emergencias que contiene el documento con la información personal.
Obligaciones:	Recabar los datos personales sin comprometer la confidencialidad de los mismos y resguardar dicha información de manera segura en la maleta de primeros auxilios de la DGRU. Mantener actualizada la información o en su caso suprimir de conformidad con la plantilla del personal activo o que se da de baja, así como por solicitud de dicho personal. Todo el proceso se realiza sin comprometer la confidencialidad de los datos personales. En caso de emergencia, poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad / Responsable sanitario

Funciones:	Mediante videoconferencia únicamente con el titular de los datos personales, recabar y capturar la información de seguimiento en la plataforma informática “Bitácora del Responsable Sanitario” del Comité de Seguimiento COVID-19, a través de un sistema de autentificación, mediante usuario y contraseña (intransferible).
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento. Registrar la información de seguimiento sanitario en la plataforma informática "Bitácora del Responsable Sanitario" así como constatar la correcta implementación de las medidas señaladas en los Lineamientos generales para el regreso a las actividades universitarias en el marco de la pandemia de COVID-19 publicados en Gaceta UNAM el 22 de junio de 2020. Realizar todo el proceso sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Tila María Pérez Ortiz
Cargo:	Directora General de Repositorios Universitarios
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.

Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Co-Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Informática
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.

Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Rubén Ignacio Sáenz González
Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Ana Laura Méndez Franco
Cargo:	Jefa de Departamento de Planeación y Seguimiento de Proyectos / Ayudante de Responsable Sanitario

Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios En caso de ausencia del Responsable Sanitario, se llevarán a cabo las funciones relacionadas con el cargo.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento. En caso de ausencia del Responsable Sanitario, se cumplirán las obligaciones del cargo asegurándose de no comprometer la confidencialidad del resto de la información contenida en los documentos.
Rinde cuentas a:	Coordinadora Planeación, Gestión y Normatividad y Dirección General
Co-Responsable	
Nombre:	Edurne Dolores Uriarte Santillán
Cargo:	Jefa de Departamento de Inventario de Colecciones y Datos de Investigación
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.

Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Co-Responsable	
Nombre:	Daniel Pérez Castillo
Cargo:	Jefe de Departamento de Datos de Investigación
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Co-Responsable	
Nombre:	Roberto Rico Chávez
Cargo:	Jefe de Departamento de Infraestructura, Centro de Datos y Servicios

Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Co-Responsable	
Nombre:	Oscar Hernández Hernández
Cargo:	Jefe de Departamento de Instalación y Soporte de Repositorios Universitarios
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargados	

Nombre:	Personal de servicios profesionales
Cargo:	No aplica
Funciones:	Poner a disposición del personal de emergencias, el documento físico con la información de contacto que se encuentra en la maleta de primeros auxilios.
Obligaciones:	Poner a disposición del personal de emergencias, la información de contacto exclusivamente para la atención de la emergencia de la persona implicada, asegurándose de no comprometer la confidencialidad del resto de la información contenida en el documento.
Rinde cuentas a:	Persona a cargo de la coordinación en que colabore y Dirección General
Usuarios	
Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

3.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único PE2	PE2

Nombre del sistema	Gestión sanitaria y emergencias
Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]

3.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
1. Fichas con datos de emergencia del personal de la DGRU. 2. Información para el seguimiento sanitario COVID-19 de la UNAM que se registra en la Bitácora de Responsable Sanitario administrada por el Comité de Seguimiento COVID-19 de la UNAM.	1. Las fichas con datos de emergencia son importantes para brindar atención médica necesaria en caso de emergencia. 2. La información registrada en la Bitácora de Responsable Sanitario es importante para dar cumplimiento a las disposiciones del Comité de Seguimiento COVID-19 de la UNAM.	1. En las fichas con datos de emergencia, se recaban nombres y número telefónico de personas para contacto en caso de emergencia, información de enfermedades o alergias para dar atención médica en caso de ser necesario. 2. La información de seguimiento de COVID-19 únicamente se comunica mediante llamada telefónica u otro medio de comunicación directo en tiempo real para su captura simultánea en la "Bitácora del Responsable Sanitario".

Dueño		
¿A quién pertenece el activo de información?		
Asistente Ejecutivo (fichas con datos de emergencia). Coordinadora de Planeación, Gestión y Normatividad / Responsable sanitario (captura simultánea de información en la "Bitácora del Responsable Sanitario"). Comité de Seguimiento COVID-19 de la UNAM (propietario y administrador de la Bitácora de Responsable Sanitario). Nota: Se excluyen los requisitos para la plataforma "Bitácora de Responsable Sanitario" debido a que no es administrada por la DGRU, sí se incluyen los requisitos para la captura de información ya que esto es realizado por el Responsable Sanitario de la DGRU de manera simultánea al recibir la información del titular de los datos personales o de un tercero facultado por el titular.		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	La información de contacto y salud únicamente es utilizada en caso de emergencia.
(X) Integridad	Solo personal autorizado puede modificar las fichas de emergencia de la manera indicada.	Los datos personales de contacto en las fichas de emergencia solo pueden ser modificados por el personal que los proporcionó. La información de seguimiento sanitario únicamente puede ser modificada por solicitud del titular de la información al responsable sanitario, quien la captura de manera simultánea al recibirla del titular de los datos personales o un tercero facultado por el titular, en la plataforma informática "Bitácora del Responsable Sanitario" a través de usuario y contraseña.

(X) Disponibilidad	Este activo debe estar disponible durante la permanencia del personal en las instalaciones de la DGRU.	La información contenida en la ficha con datos de emergencia (datos personales y de salud) está disponible para consulta del personal únicamente en caso de emergencia.
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
(X) Confidencialidad	**( ) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]

EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]

3.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Gestión sanitaria y emergencias

[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					

[redacted]				[redacted]	

CONTENEDORES FÍSICOS

[redacted]			
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		
[redacted]		[redacted]	[redacted]

[redacted]			
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

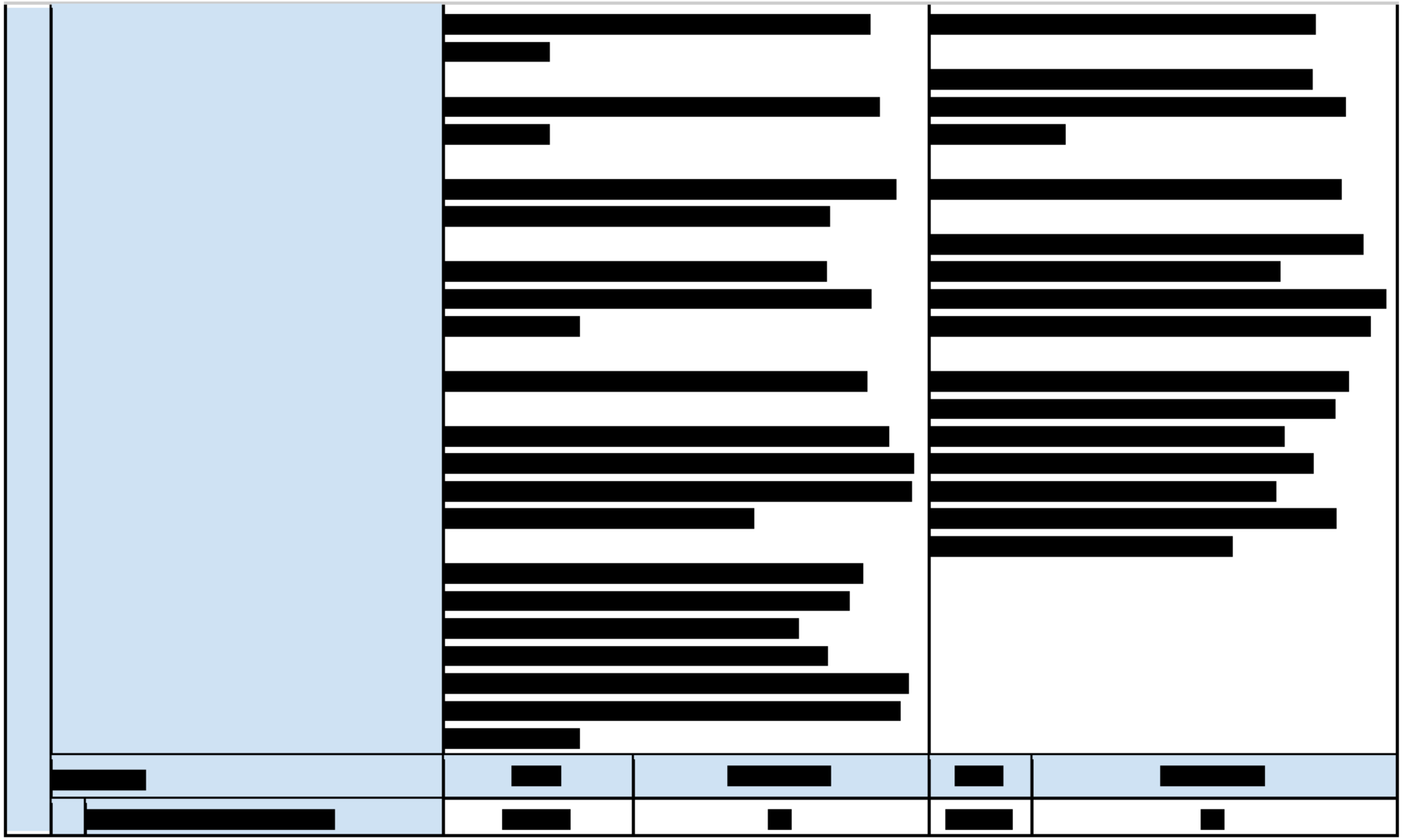
RECURSOS HUMANOS

[redacted]

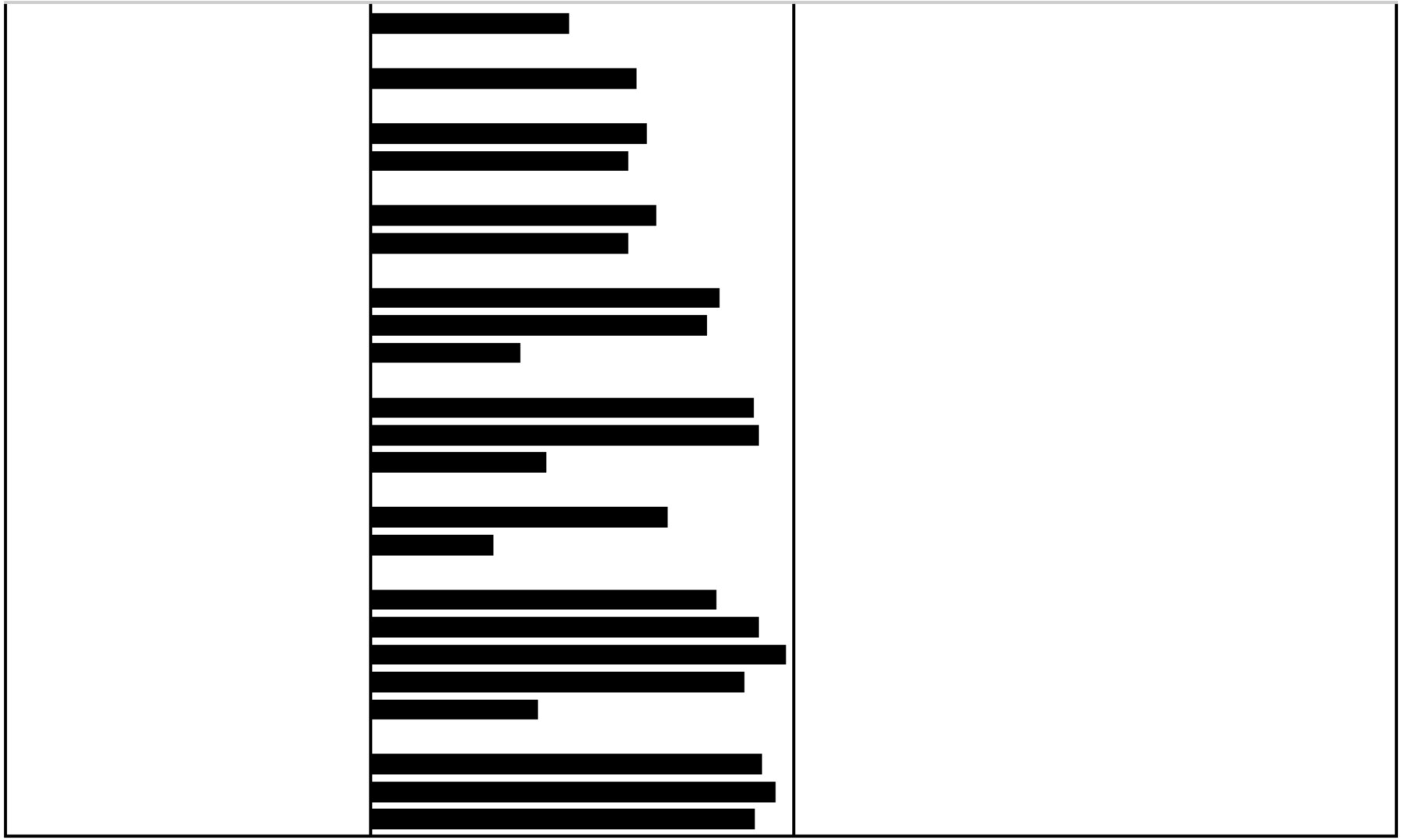
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

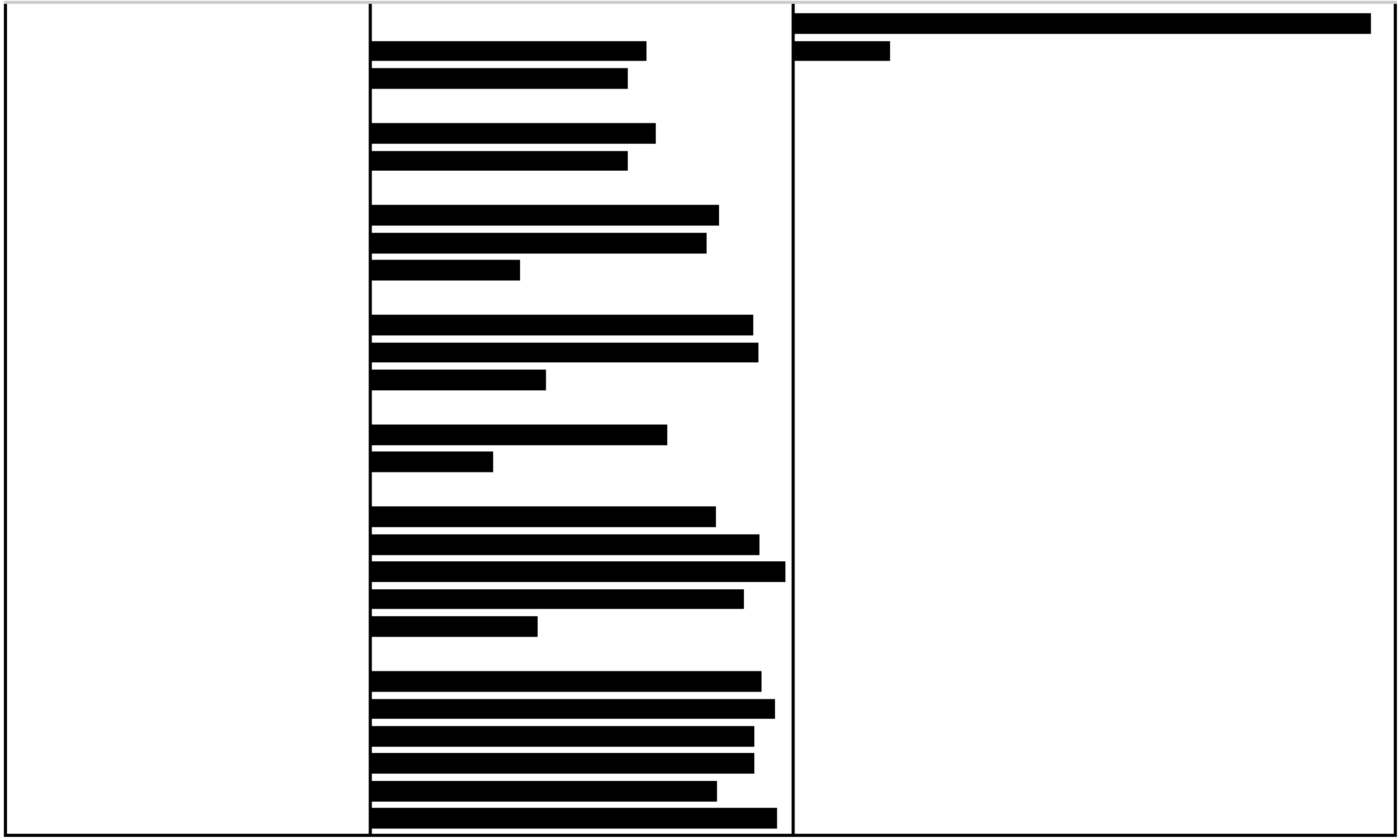
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

3.5. ANÁLISIS DE RIESGOS



Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión Sanitaria y Emergencias	
ANÁLISIS DE RIESGOS		
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]





	[redacted]	

3.6. ANÁLISIS DE BRECHA

Dirección General, DGRU			
Identificador único	PE2		
Nombre del sistema PE2	Gestión sanitaria y emergencias		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		

[redacted]	[redacted]	[redacted]	[redacted]

3.7. PLAN DE TRABAJO

Dirección General, DGRU				
Identificador único	PE2			
Nombre del sistema PE2	Gestión sanitaria y emergencias			
Actividad	**Descripción**	**Duración**	**Cobertura**	Prioridad
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

3.8. MEDIDAS DE SEGURIDAD

Dirección General, DGRU

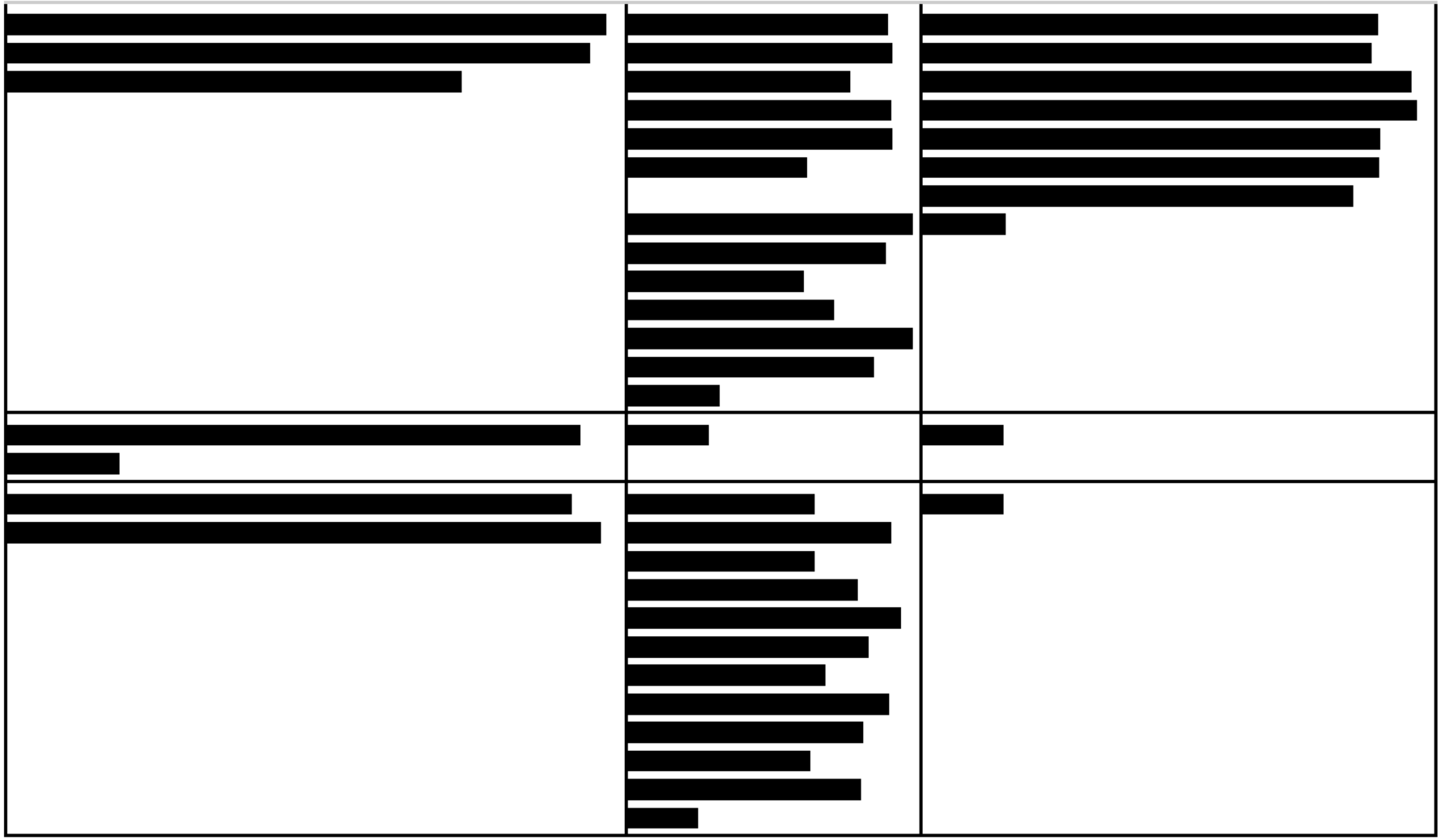
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	PE2
Nombre del sistema PE2	Gestión sanitaria y emergencias
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	
[redacted]	
[redacted]	
[redacted]	

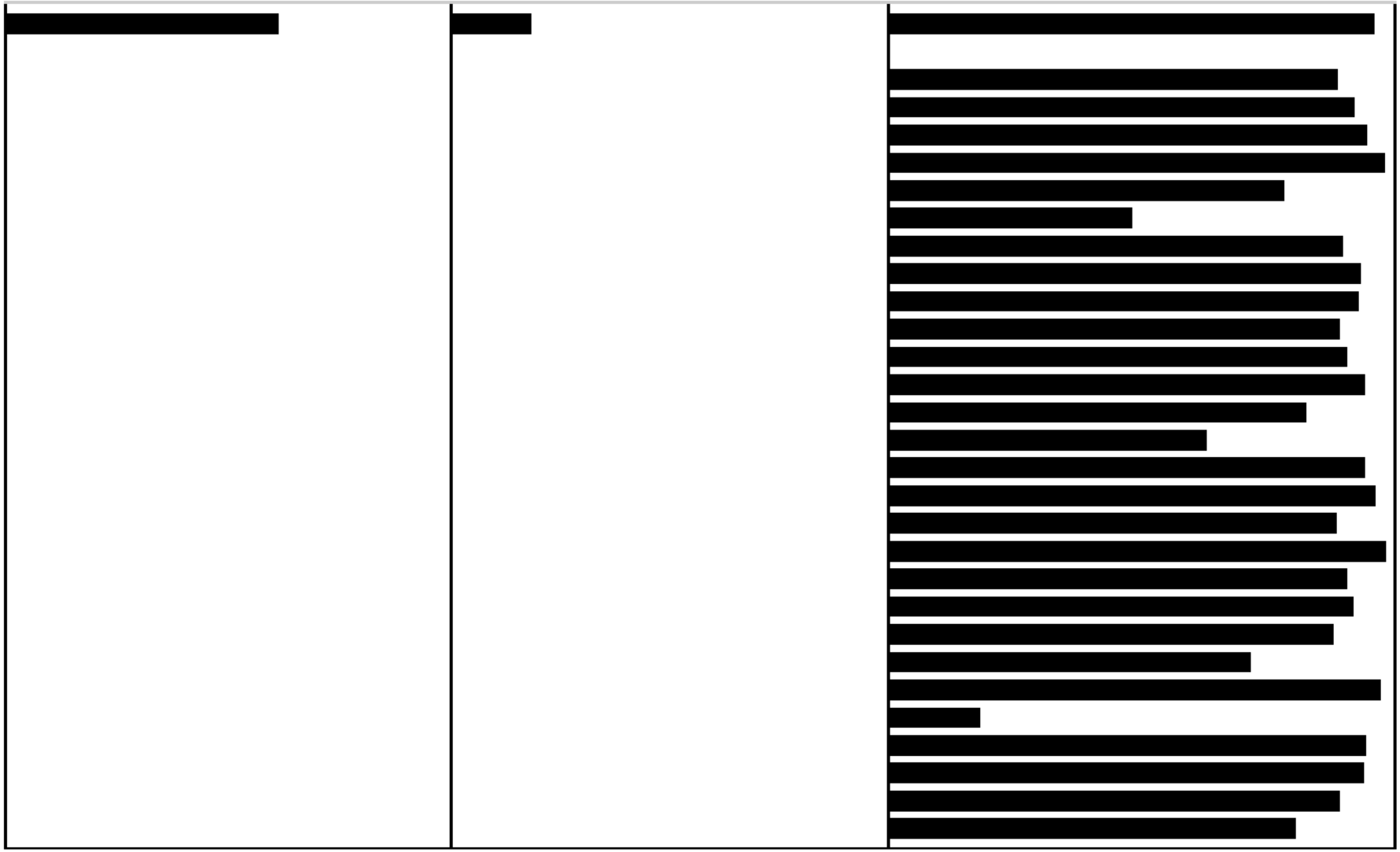
[redacted]

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		



[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

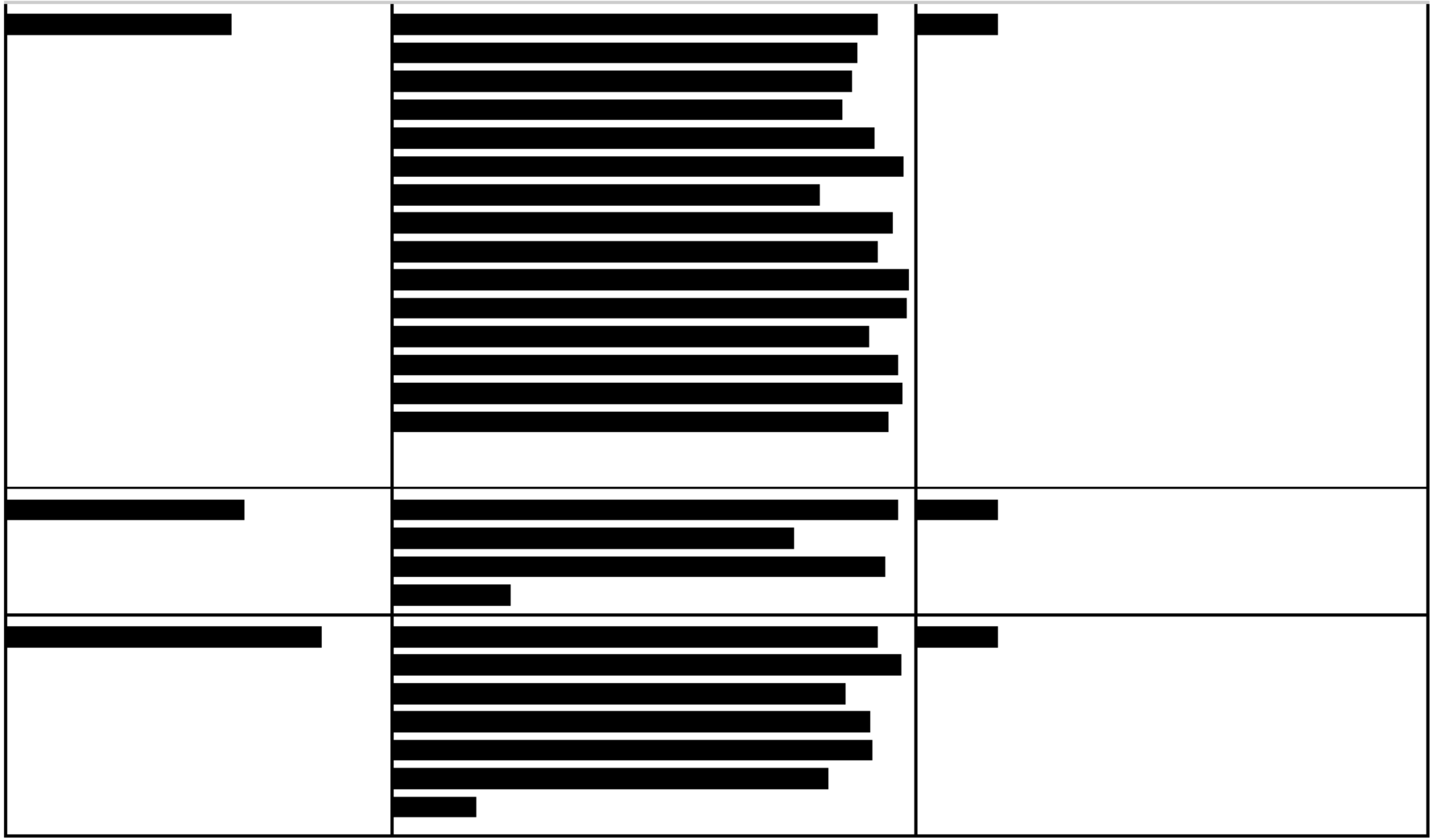
Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
	[redacted]	[redacted]
[redacted]		

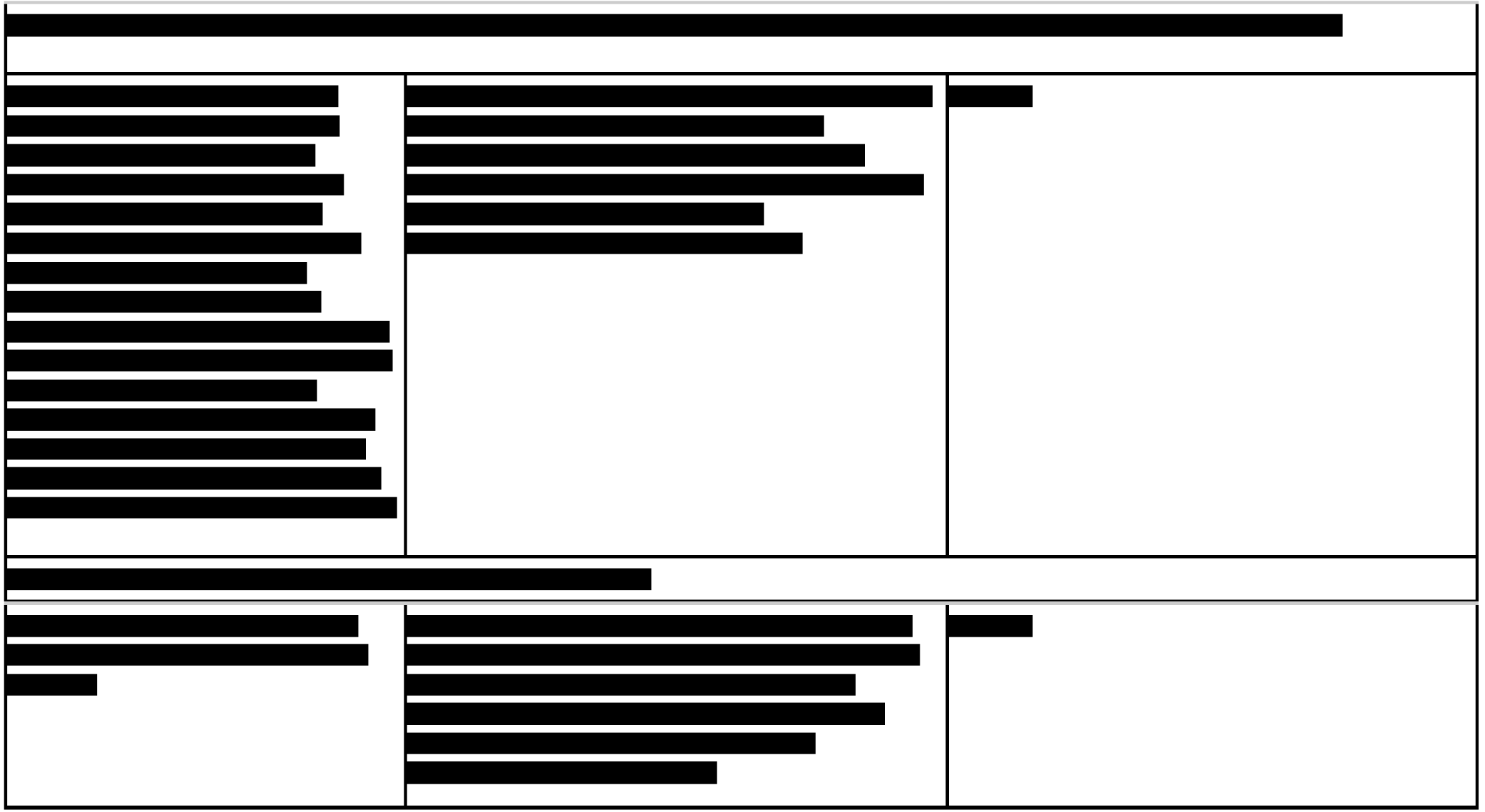


		[redacted]

[redacted]		
	[redacted]	[redacted]

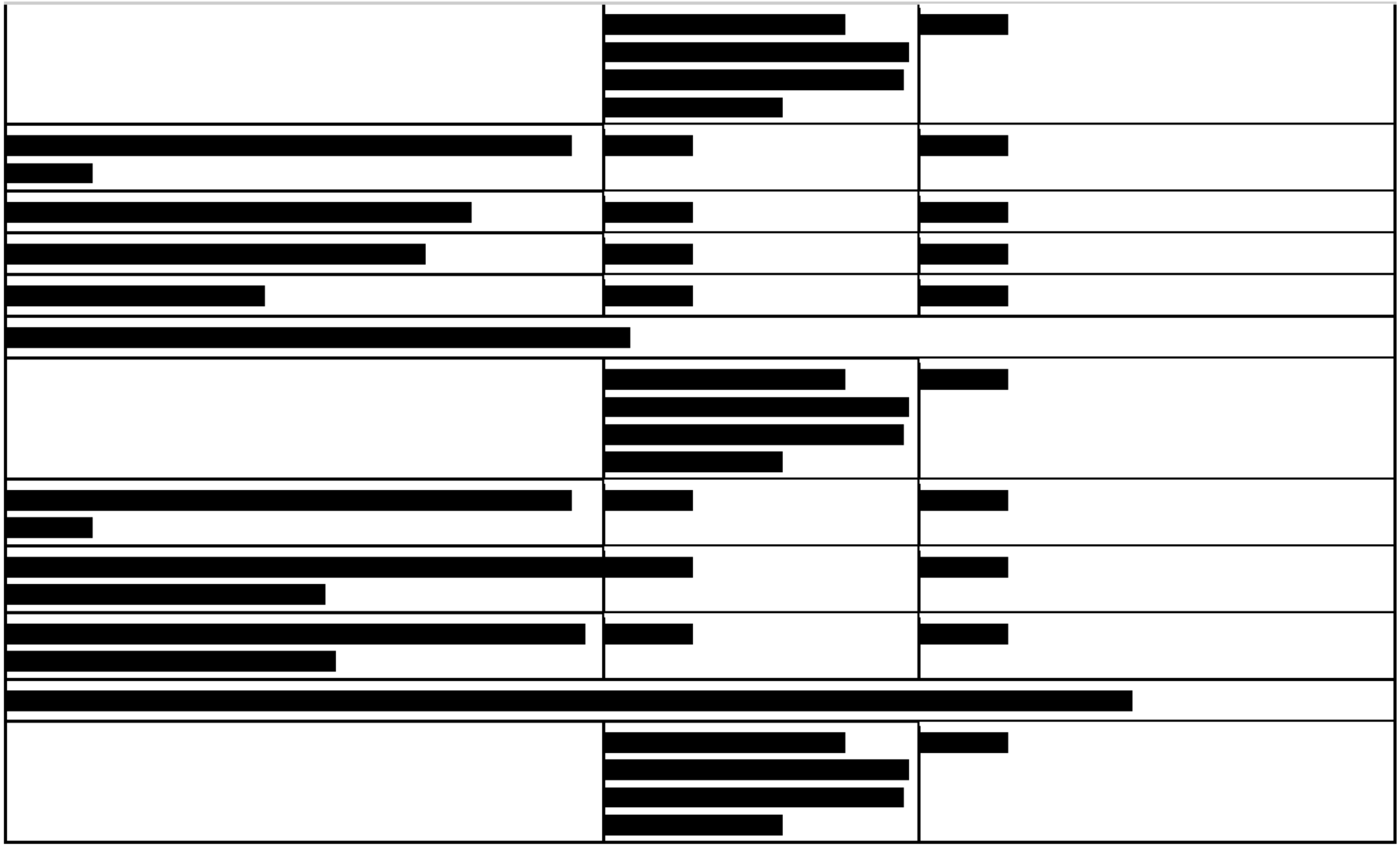
Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]





Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		



Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]		
[redacted]		
[redacted]		

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]		
[redacted]		

3.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
Recurso	**Descripción**	**Control**

[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General, DGRU	
Identificador único	PE2
Nombre del sistema PE2	Gestión sanitaria y emergencias

Medida de seguridad	Resultado de evaluación	Responsable
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Dirección General, DGRU		
Identificador único	PE2	
Nombre del sistema PE2	Gestión sanitaria y emergencias	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]

3.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU	
Identificador único	PE2
Nombre del sistema PE2	Gestión sanitaria y emergencias

Actividad	Descripción	Duración	Cobertura	Prioridad
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Dirección General, DGRU				
Identificador único	PE2			
Nombre del sistema PE2	Gestión sanitaria y emergencias			
Actividad	Descripción	Duración	Cobertura	Prioridad
Desarrollar un programa de difusión de la protección a los datos personales y el	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente	Sesiones variables,	Todo el personal de DGRU.	Alta

material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales, - Procedimientos de borrado seguro de correos electrónicos y de archivos; - Uso adecuado de sesiones en la plataforma y en los equipos del personal, así como del uso adecuado de la plataforma "Bitácora del Responsable Sanitario" para evitar accesos indebidos.	agendadas para revisar el material generado para este fin.	dependiendo de los temas a tratar.	Frecuencia de la actualización una vez al año o antes si se considera necesario.	

Anexo 4. DG1 Contraseñas de gestión administrativa

4.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: nombre completo. 1b. Datos laborales: correo electrónico institucional, teléfono institucional, usuarios, contraseñas.	
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X)	
¿Para qué se usan?	Para el acceso a sistemas externos a la DGRU de gestión administrativa en la UNAM.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal ( )	Gobierno Estatal ( ) Gobierno Municipal ( ) Personas físicas ( ) Personas morales ( ) Áreas Universitarias ( ) Personal de la misma Área Universitaria (X) Los usuarios y contraseñas se comparten sólo con personal autorizado dentro de la misma Área Universitaria, para llevar a cabo una actividad encomendada de gestión administrativa.
¿Dónde se alojan?	[redacted]	

	[redacted]
¿Cuánto tiempo se da tratamiento?	El documento estará sujeto a lo establecido en los Instrumentos de Control y Consulta Archivística de la UNAM vigentes.
Responsable	
Nombre:	Tila María Pérez Ortíz
Cargo:	Directora General
Funciones:	Recibe y comunica la información de usuario y contraseñas de acceso a sistemas externos a la DGRU de gestión administrativa en la UNAM.
Obligaciones:	Durante el proceso de recepción y comunicación de la información, se asegura que se comuniquen sólo al personal autorizado.
Co-Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad
Funciones:	Recibe, valida, usa y comunica la información de usuario y contraseñas de acceso a sistemas externos a la DGRU de gestión administrativa en la UNAM.
Obligaciones:	Durante todo el proceso de recepción, validación, uso, comunicación y resguardo de las contraseñas de gestión administrativas, se asegura de que se comuniquen sólo al personal autorizado; que se resguarde de manera correcta de acuerdo a los procedimientos internos de la DGRU y de acuerdo a los Instrumentos de Control y Consulta Archivística de la UNAM, así como de que se mantenga la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Nombre:	Ana Laura Méndez Franco
Cargo:	Jefa de Departamento de Planeación y Seguimiento de Proyectos
Funciones:	Uso y resguardo de contraseñas para acceder a los sistemas externos a la DGRU de gestión administrativa de la UNAM.
Obligaciones:	Durante todo el proceso de uso y resguardo de las contraseñas se asegura de que los documentos relacionados sean clasificados y archivados de manera correcta de acuerdo con los procedimientos internos de la DGRU y de acuerdo a los Instrumentos de Control y Consulta Archivística de la UNAM, así como de que se mantenga la confidencialidad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Encargados	
Nombre:	Alejandro Chávez Méndez
Cargo:	No aplica
Funciones:	Resguardar de manera segura los datos personales contenidos en los documentos físicos y digitales relacionados con usuarios y contraseñas para acceder a los sistemas externos a la DGRU de gestión administrativa de la UNAM.
Obligaciones:	Digitalizar los documentos que contengan los usuarios y contraseñas, asegurando la integridad de dichos datos personales. Archivar el documento digital en un espacio encriptado en la DGRU. Archivar el documento físico, en caso de existir, conforme a los procedimientos internos de la DGRU y a los Instrumentos de Control y Consulta Archivística de la UNAM. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Usuarios	
Nombre:	No aplica

Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

4.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	DG1
Nombre del sistema DG1	Contraseñas de gestión administrativa
Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]

4.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Documentos y correos electrónicos que incluyen usuario y contraseña de acceso a diversos portales de gestión administrativa institucional	Porque se utilizan diversos portales institucionales de gestión administrativa cuya información es de acceso confidencial.	Documentos y correos electrónicos con datos personales, laborales e información de acceso de la persona responsable de ingresar a las plataformas de gestión administrativa.
Dueño		
¿A quién pertenece el activo de información?		
Directora General		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	Solo la titular y la(s) persona(s) designadas por ella, podrán acceder al oficio o al correo electrónico con la información.
(X) Integridad	Solo personal autorizado puede modificar este activo de información de la siguiente manera:	La información no puede ser modificada por personal de la DGRU, únicamente por la entidad universitaria que la emite.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera:	La versión digital y física de los documentos que contienen la información deben estar disponibles únicamente para que el personal designado lo consulte.

	Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	
( ) Otro		
Requisitos de seguridad más importante		
¿Cuál es el requisito de seguridad más importante para este activo?		

(X) Confidencialidad	**( ) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]

	DGRU.
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

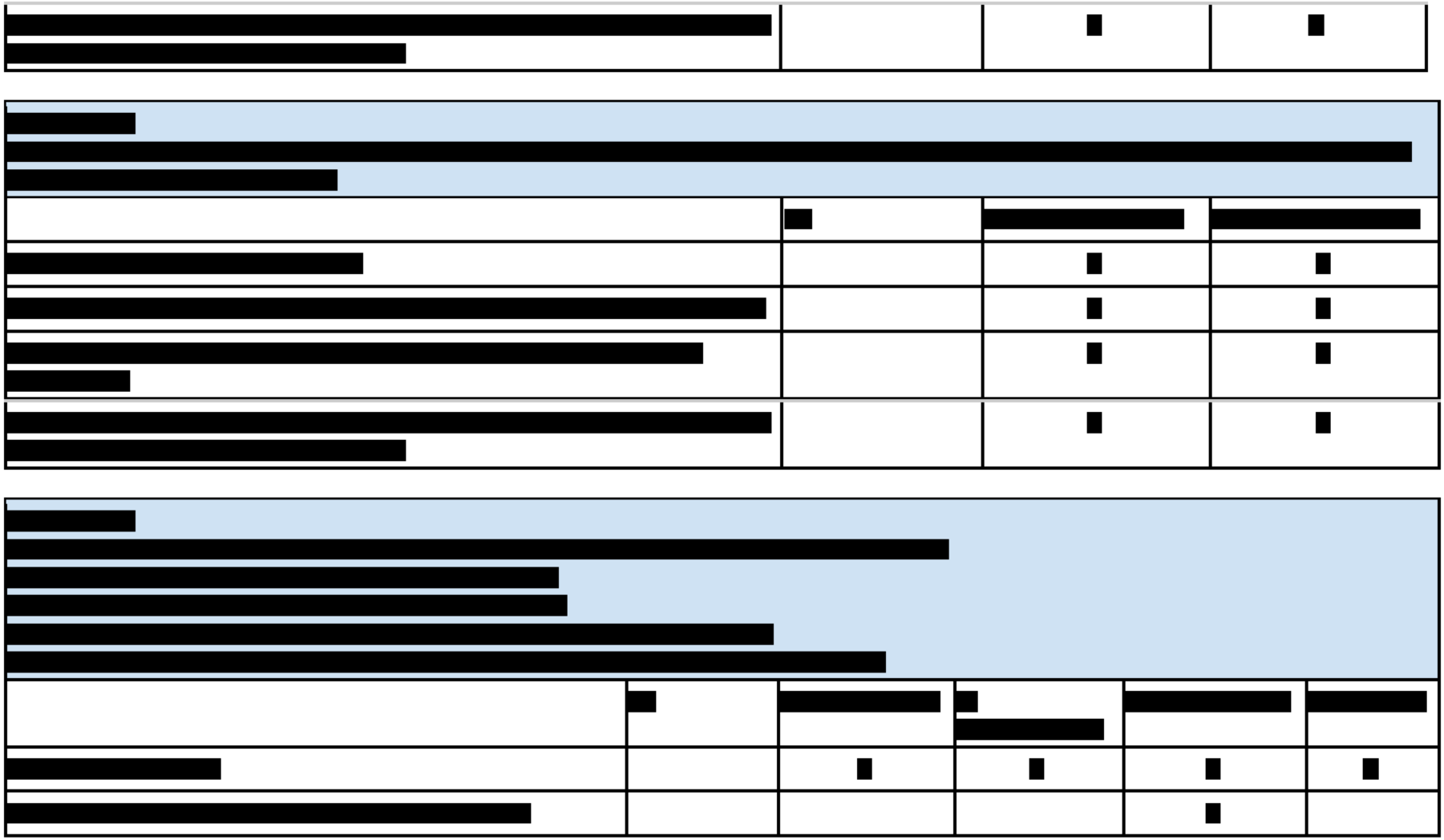
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	

4.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Contraseñas de gestión administrativa
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

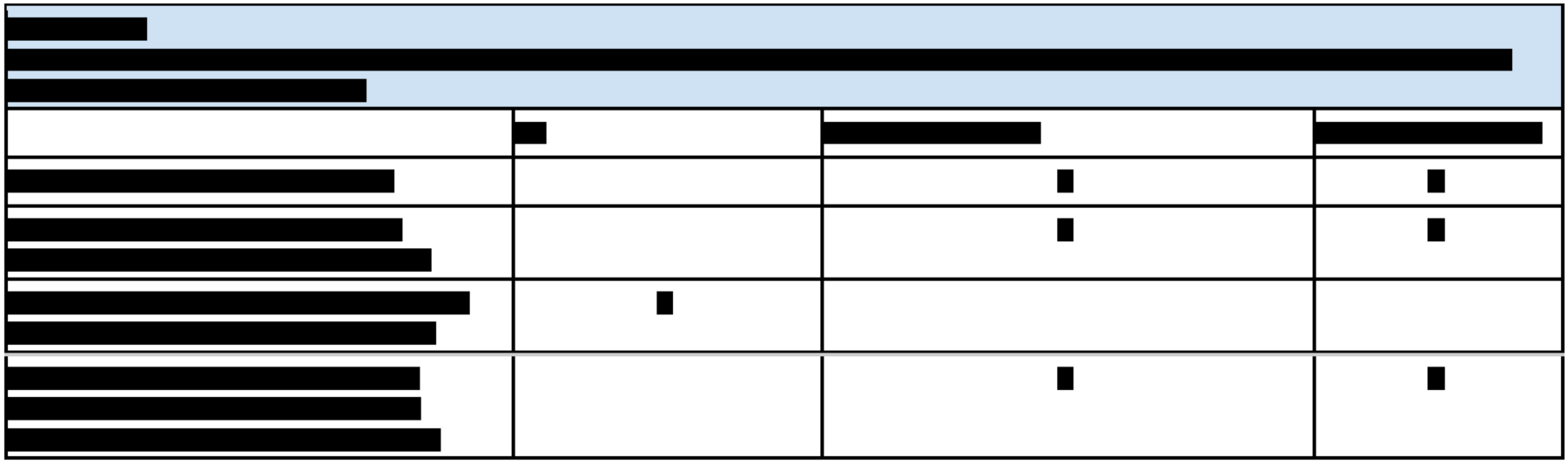
[redacted]			
[redacted]			
[redacted]			
[redacted]			



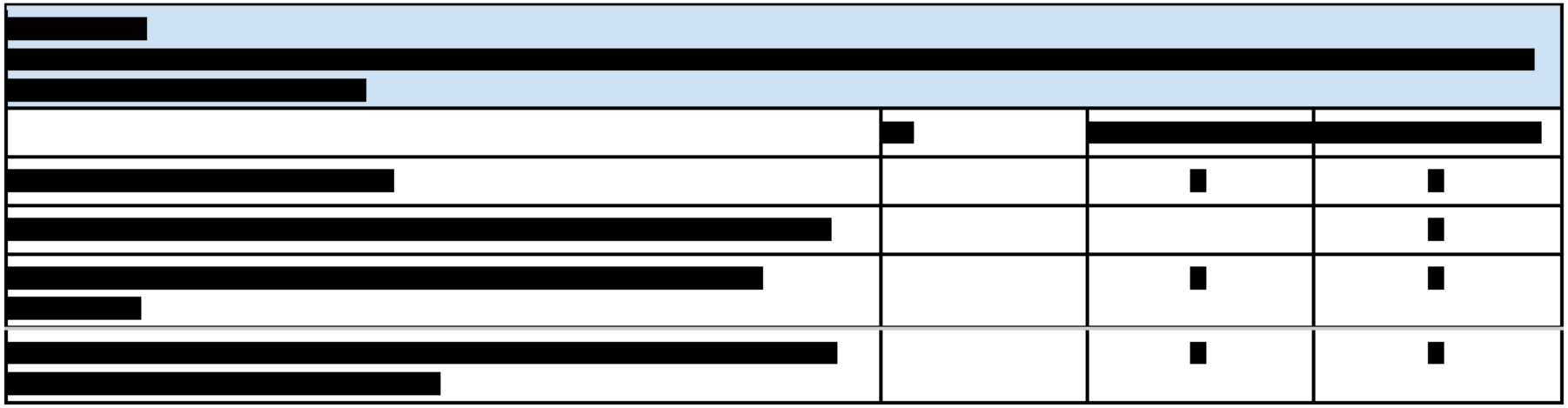
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]		[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]				[redacted]	
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			[redacted]	[redacted]	[redacted]

CONTENEDORES FÍSICOS

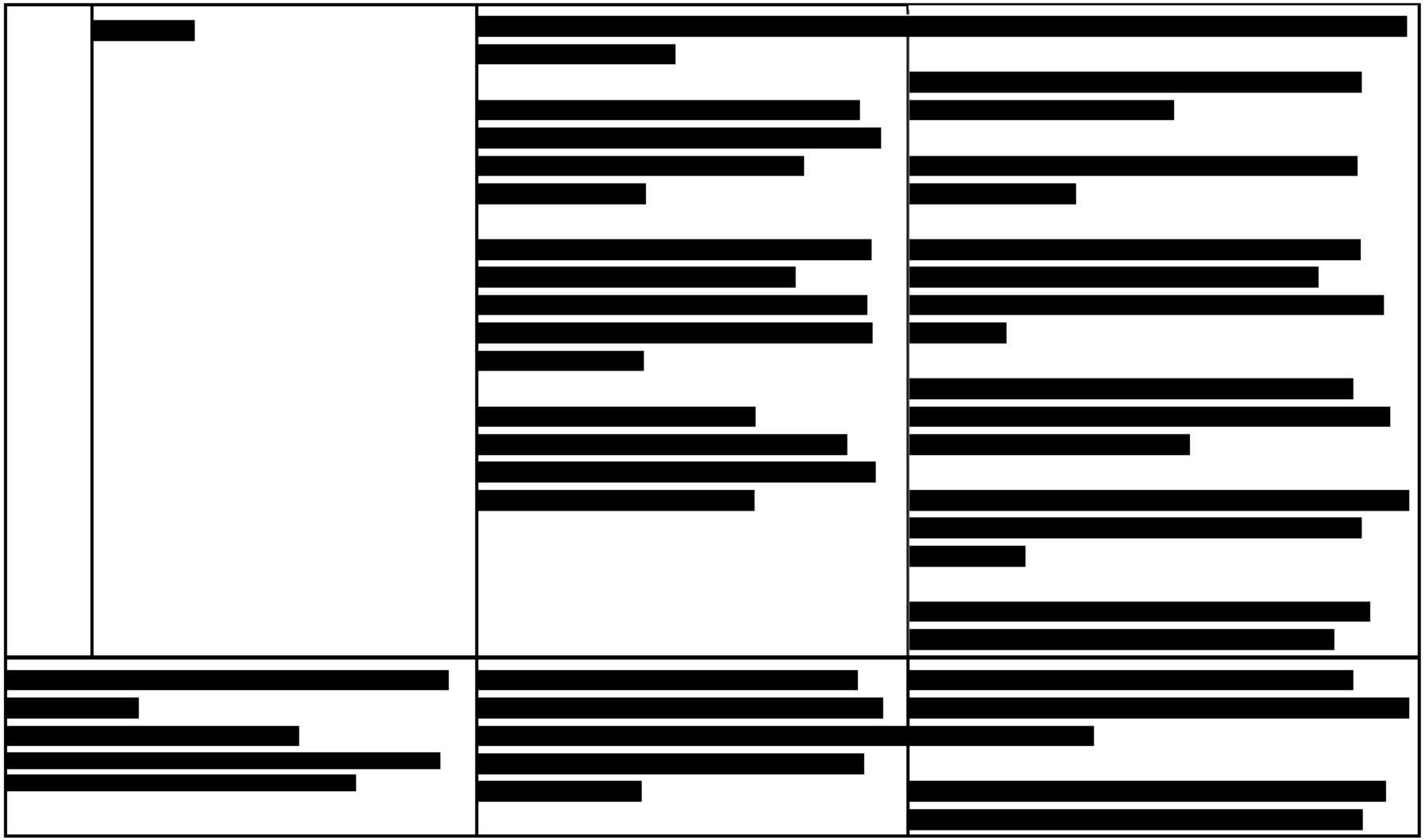
[redacted]			
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		
[redacted]		[redacted]	[redacted]



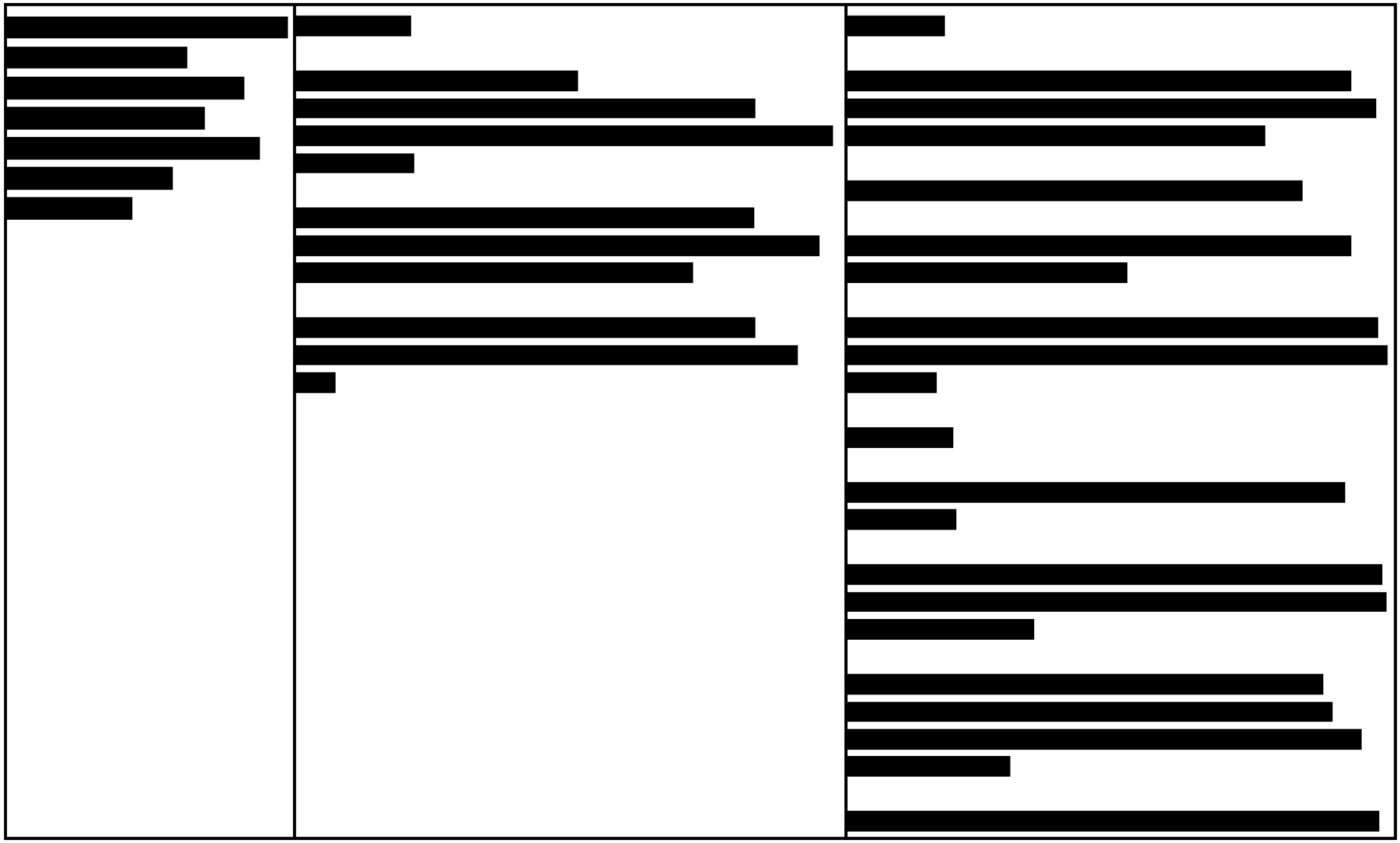
RECURSOS HUMANOS

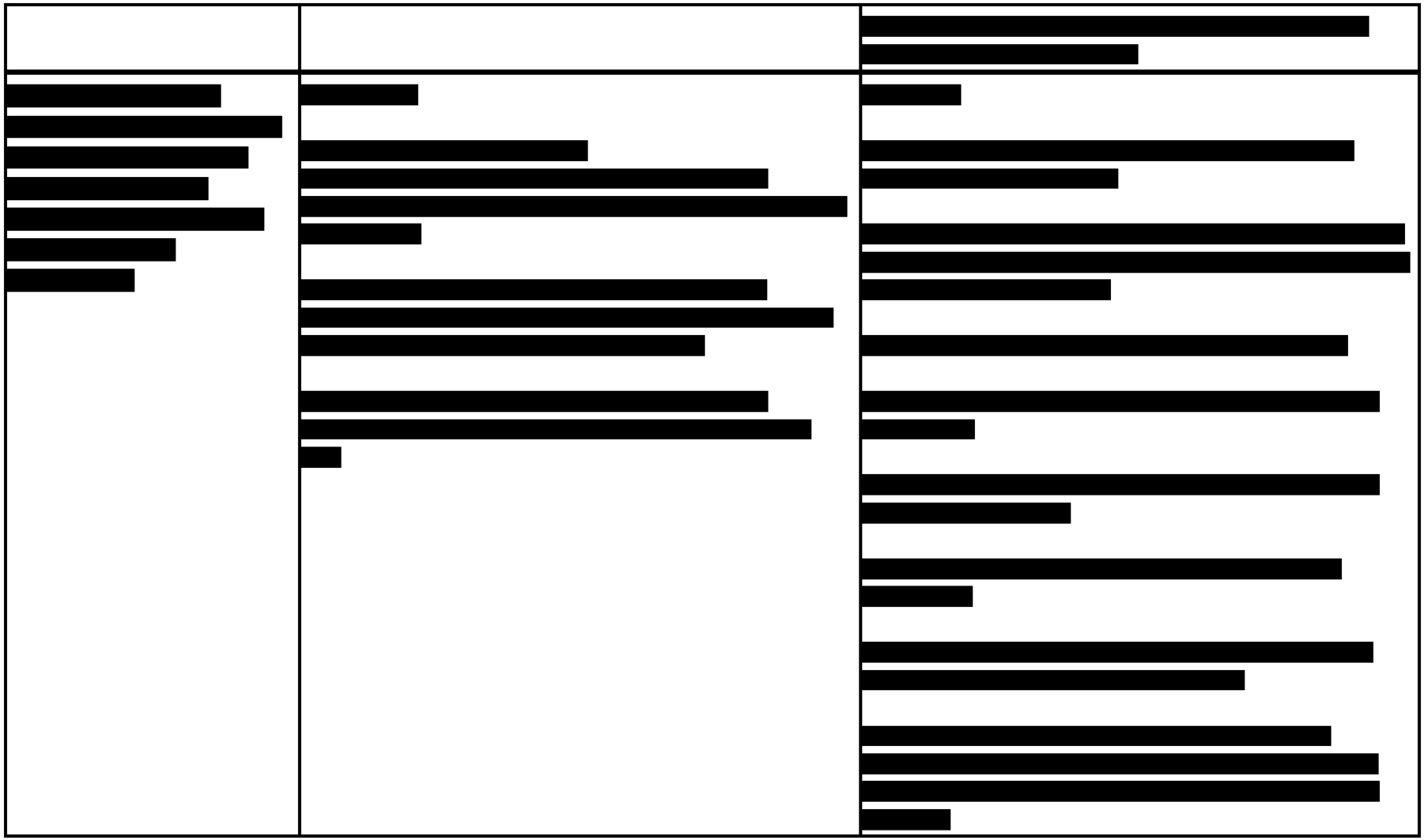


5.5. ANÁLISIS DE RIESGOS



Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de Gestión Administrativa	
ANÁLISIS DE RIESGOS		
Riesgo	**Impacto**	**Mitigación**





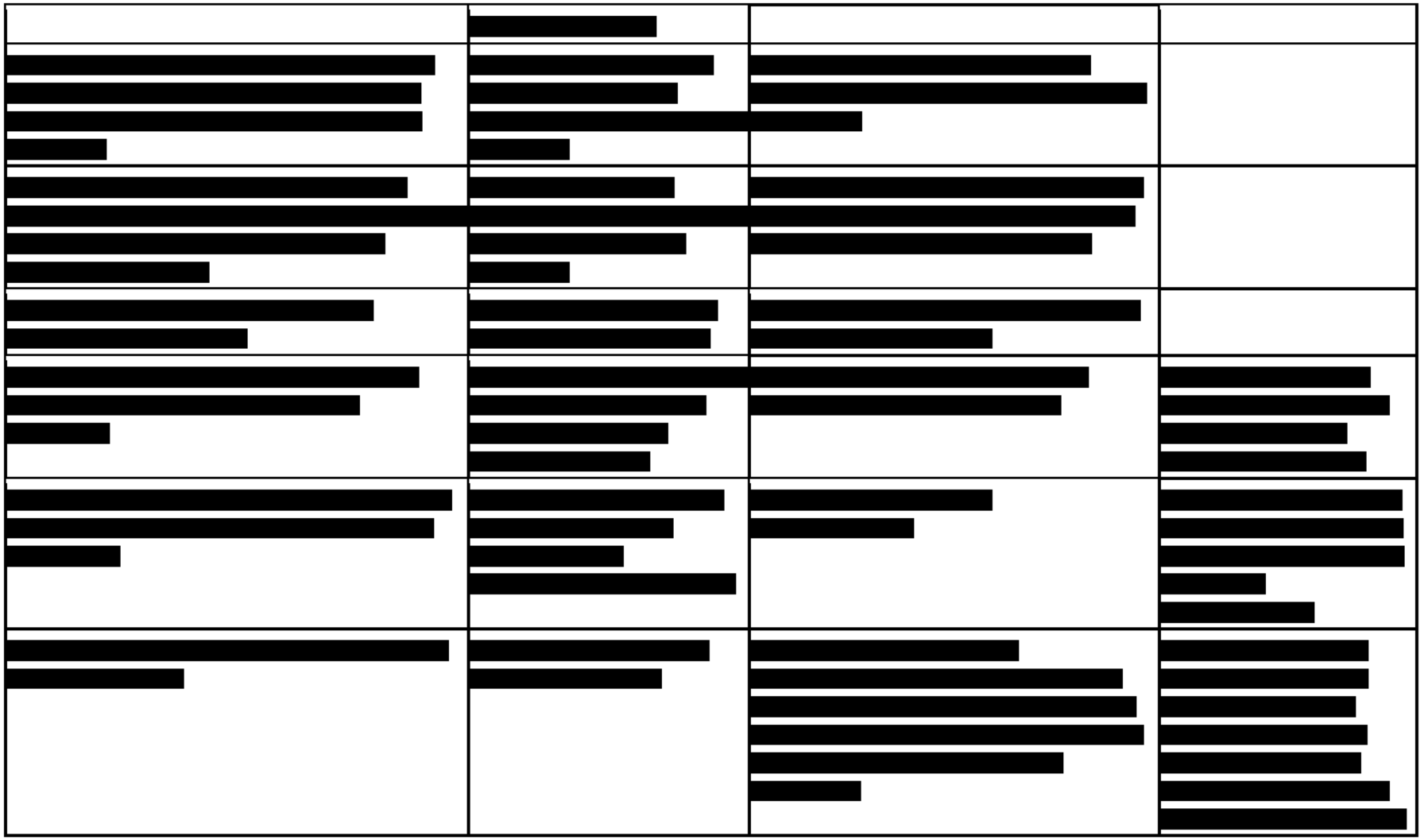
		[redacted]

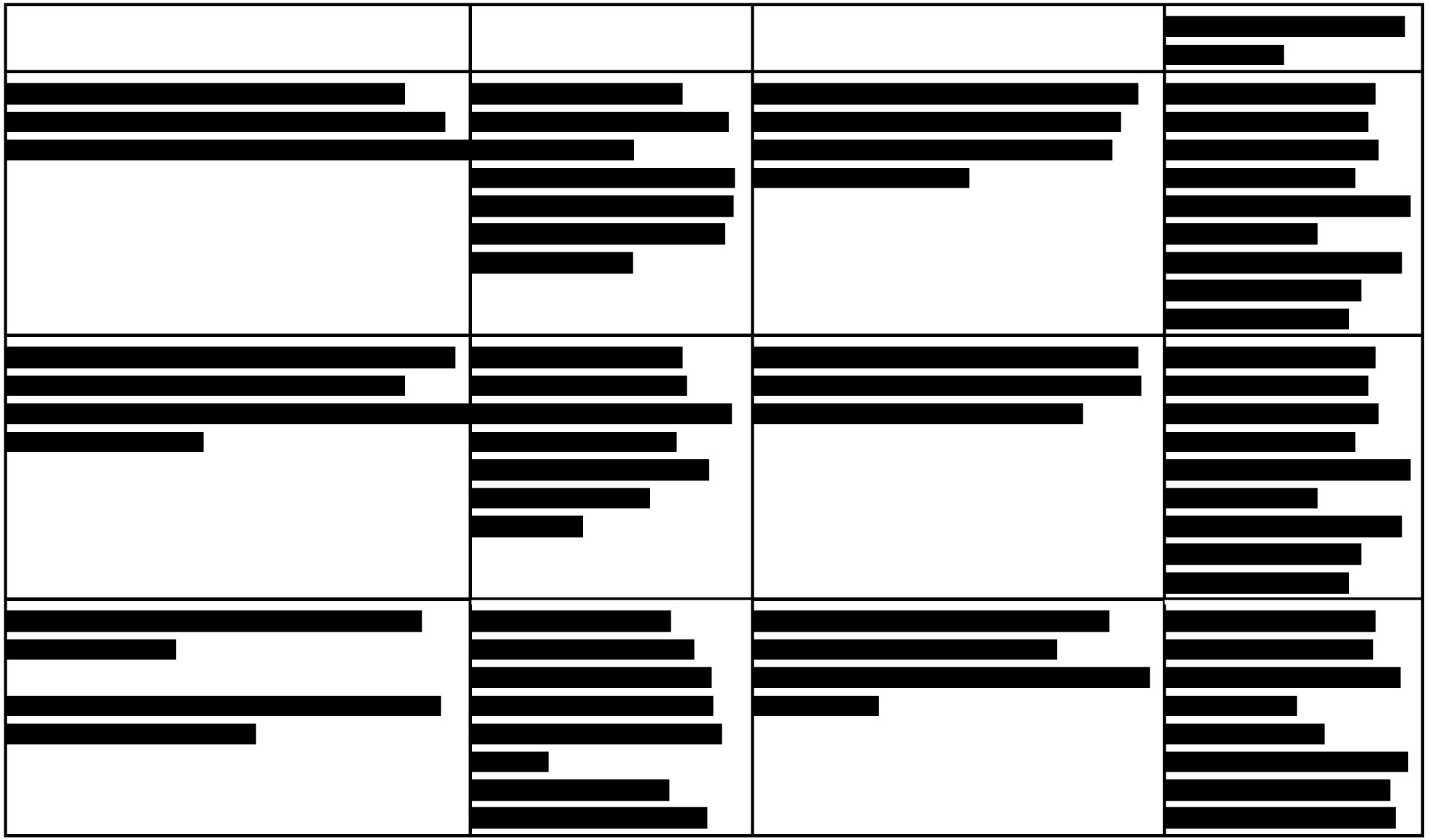
		[redacted]

4.6. ANÁLISIS DE BRECHA

Dirección General, DGRU			
Identificador único	DG1		
Nombre del sistema DG1	Contraseñas de gestión administrativa		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		





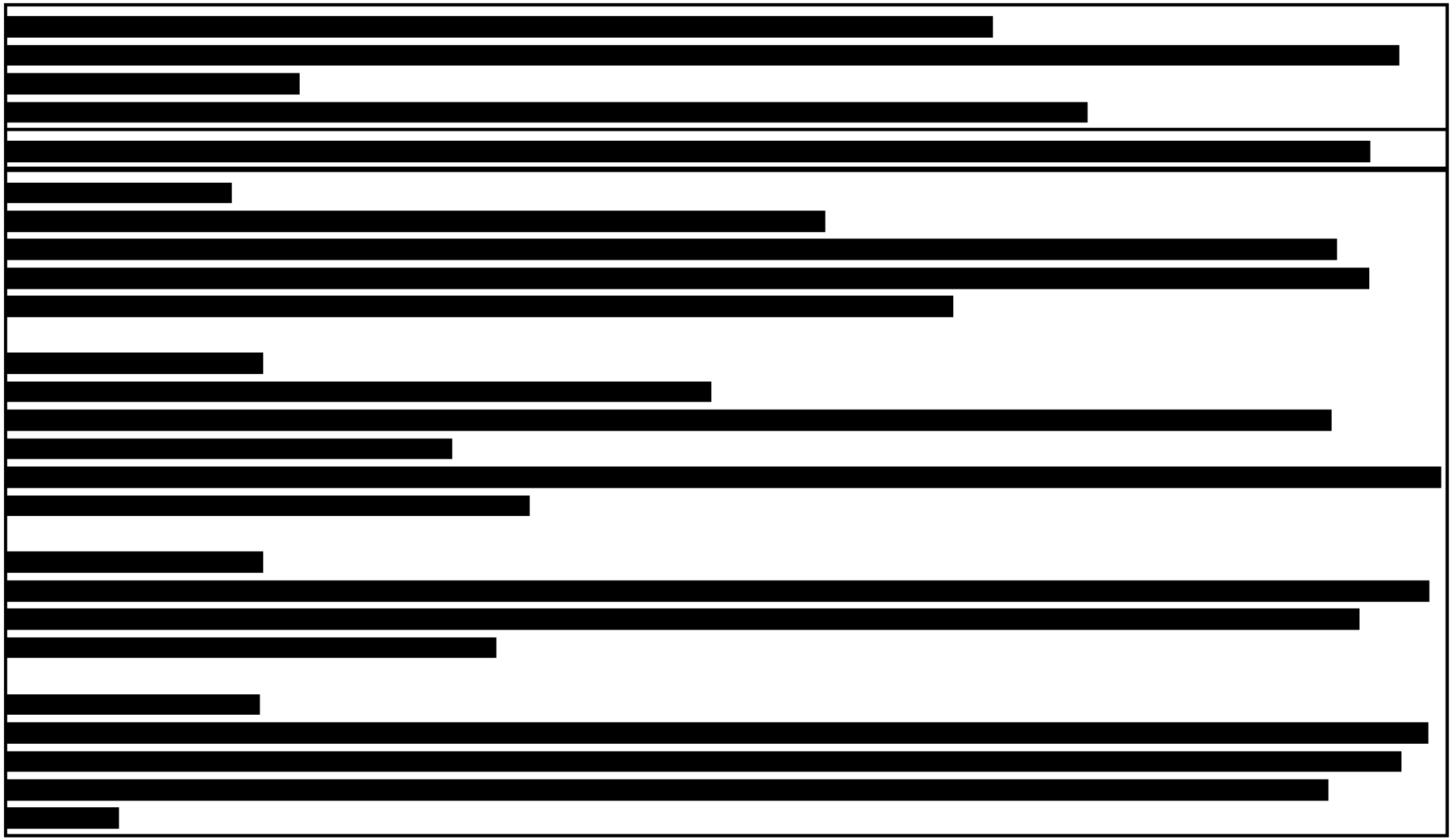
4.7. PLAN DE TRABAJO

Dirección General, DGRU				
Identificador único	DG1			
Nombre del sistema DG1	Contraseñas de gestión administrativa			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

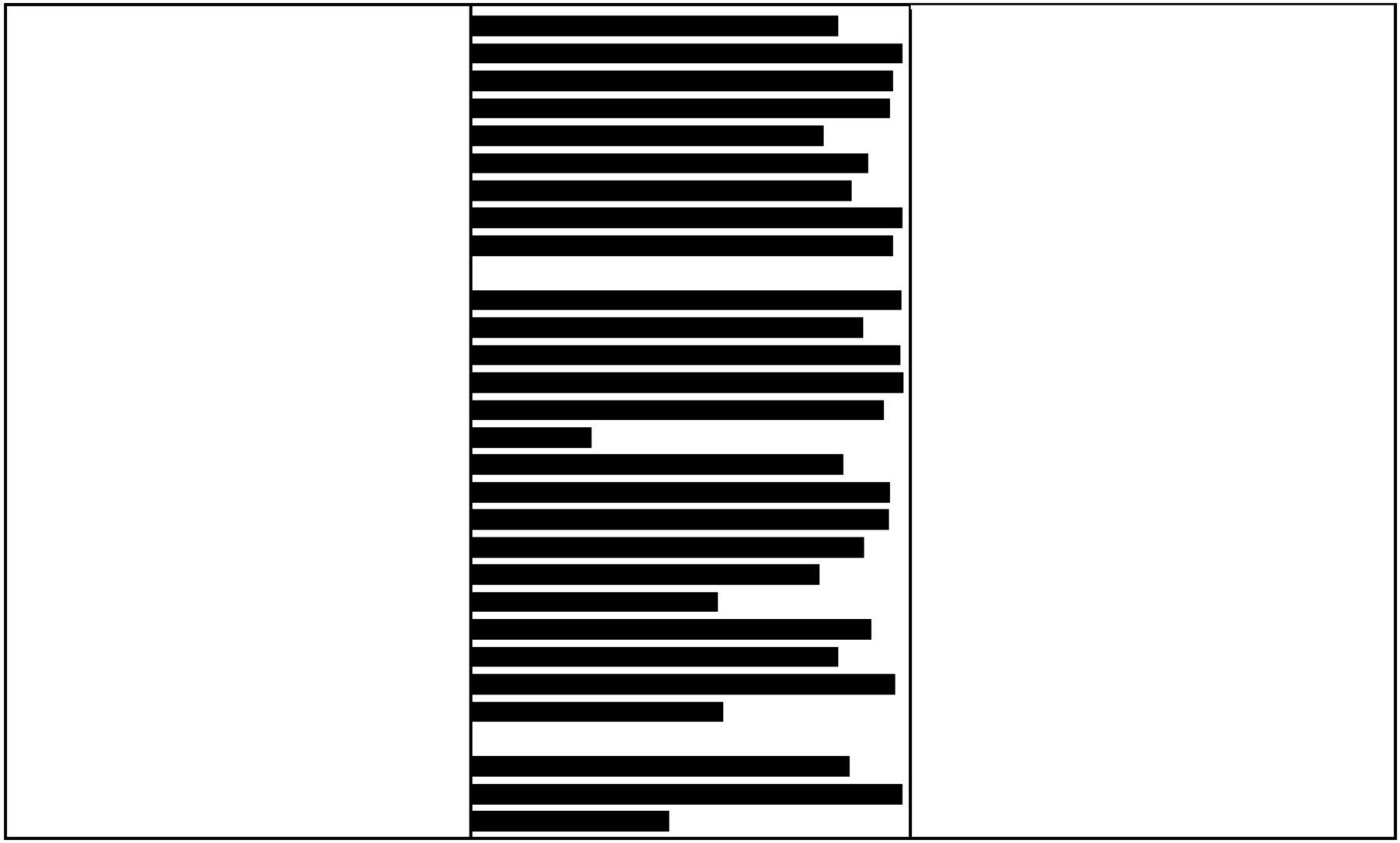
4.8. MEDIDAS DE SEGURIDAD

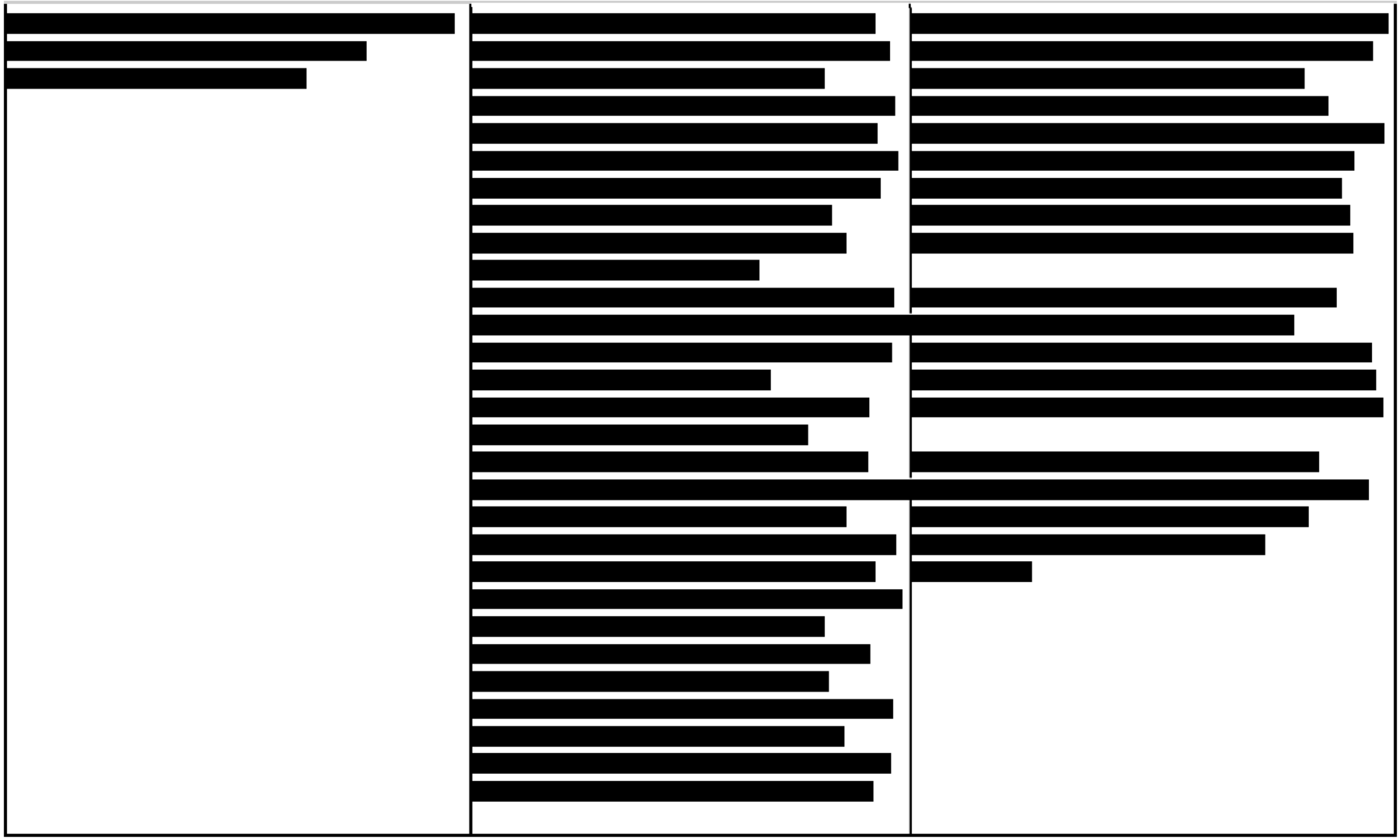
Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Dirección General, DGRU	
Identificador único	DG1
Nombre del sistema DG1	Contraseñas de gestión administrativa
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	



Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]





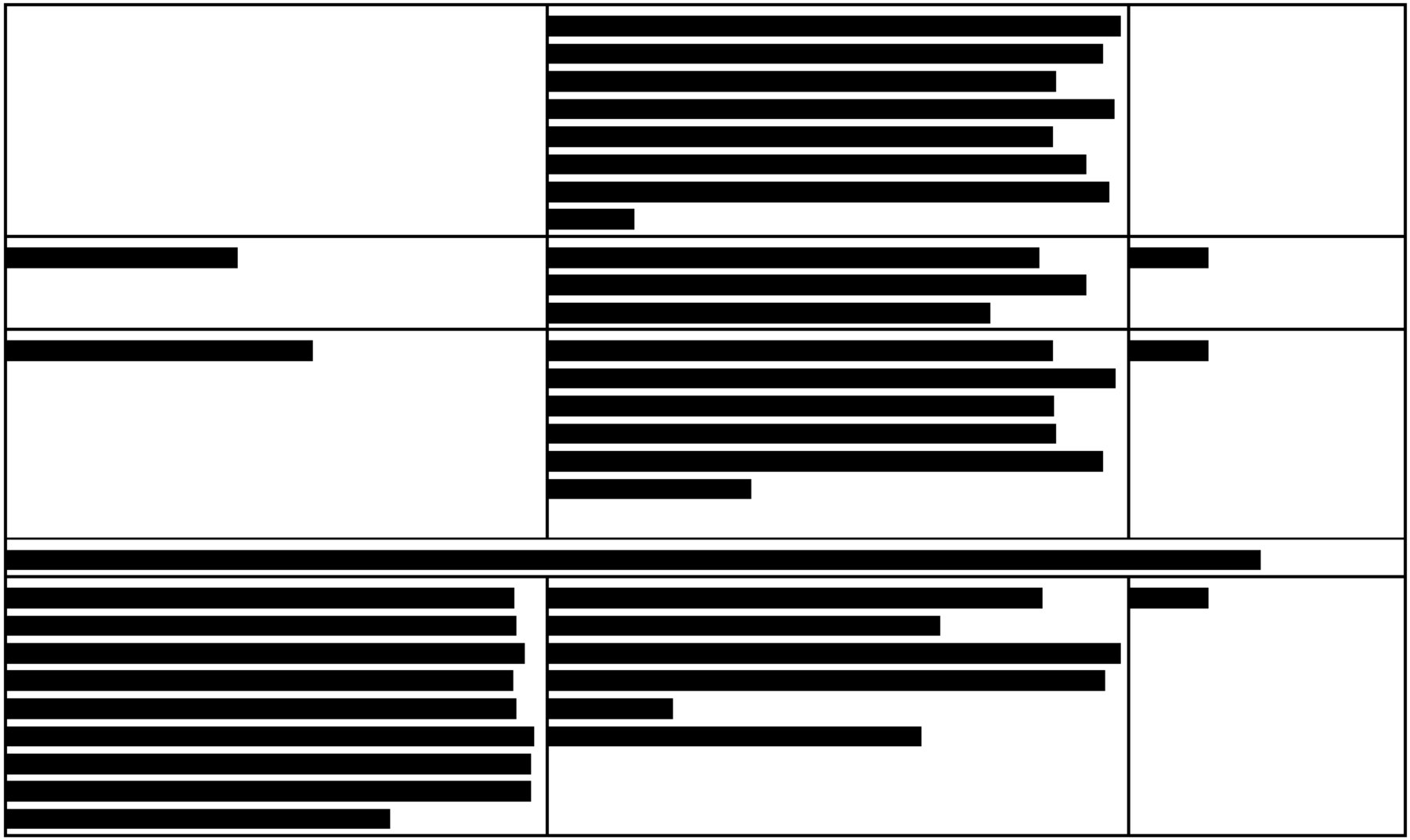
[redacted]	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]

[redacted]		
	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]



[redacted]		

Dirección General, DGRU	
Identificador único	DG1
Nombre del sistema DG1	Contraseñas de gestión administrativa
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES	

	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		

Dirección General, DGRU	
Identificador único	DG1
Nombre del sistema DG1	Contraseñas de gestión administrativa
VII. PERFILES DE USUARIO Y CONTRASEÑAS	

	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]

[redacted]		

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		

[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
Medida de seguridad	**Resultado de evaluación**	**Responsable**

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Dirección General, DGRU		
Identificador único	DG1	
Nombre del sistema DG1	Contraseñas de gestión administrativa	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU				
Identificador único	DG1			
Nombre del sistema DG1	Contraseñas de gestión administrativa			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Dirección General, DGRU	
Identificador único	DG1

Nombre del sistema DG1	Contraseñas de gestión administrativa			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales. - Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Procedimientos de borrado seguro de correos electrónicos y de archivos. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar	Personal de las coordinaciones de Desarrollo Tecnológico e Infraestructura, de Planeación, Gestión y Normatividad y de la Dirección General. Frecuencia de la actualización una vez al año o antes si se considera necesario.	Alta

Anexo 5. DG2 Formatos de gestión interna

5.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: nombre completo. 1b. Datos laborales: institución, puesto, correo electrónico institucional, teléfono institucional.	
¿Cómo se obtienen los datos personales?	Físico (X) Digital (X)	
¿Para qué se usan?	El nombre completo, institución, puesto, correo electrónico institucional y teléfono institucional, se incluyen en minutas internas y externas, formatos donde se lleva un registro de atención a usuarios de las plataformas digitales que administra la DGRU y formatos de capacitación.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal (X)	Gobierno Estatal (X) Gobierno Municipal (X) Personas físicas (X) Personas morales (X) Áreas Universitarias (X) Los datos personales incluidos en la minutas, se comparten con los asistentes a la reunión, en cuyo caso podrían ser personal interno o externo a la Universidad, dependiendo con qué entidad se lleve a cabo la reunión. También se comparten con otras áreas universitarias a las que se rinde cuenta de las actividades que realiza la DGRU.

		Los datos personales incluidos en los formatos de registro de atención a usuarios de las plataformas digitales que administra la DGRU y formatos de capacitación se comparten con otras áreas universitarias a las que se rinde cuenta de las actividades que realiza la DGRU.
¿Dónde se alojan?	[redacted]	
¿Cuánto tiempo se da tratamiento?	La disposición de documentos es el establecido en los Instrumentos de Control y Consulta Archivística de la UNAM vigentes.	
Responsable		
Nombre:	Tila María Pérez Ortiz	
Cargo:	Directora General de Repositorios Universitarios	
Funciones:	Recabar, registrar y revisar los datos personales en las minutas.	
Obligaciones:	Compartir las minutas con los asistentes. Enviar a resguardo en Sistema Documental de la DGRU dicho documento físico o digital. Realizar el proceso sin comprometer la integridad de los datos personales.	
Responsable		
Nombre:	Ariana Chávez Méndez	
Cargo:	Coordinadora de Planeación, Gestión y Normatividad	

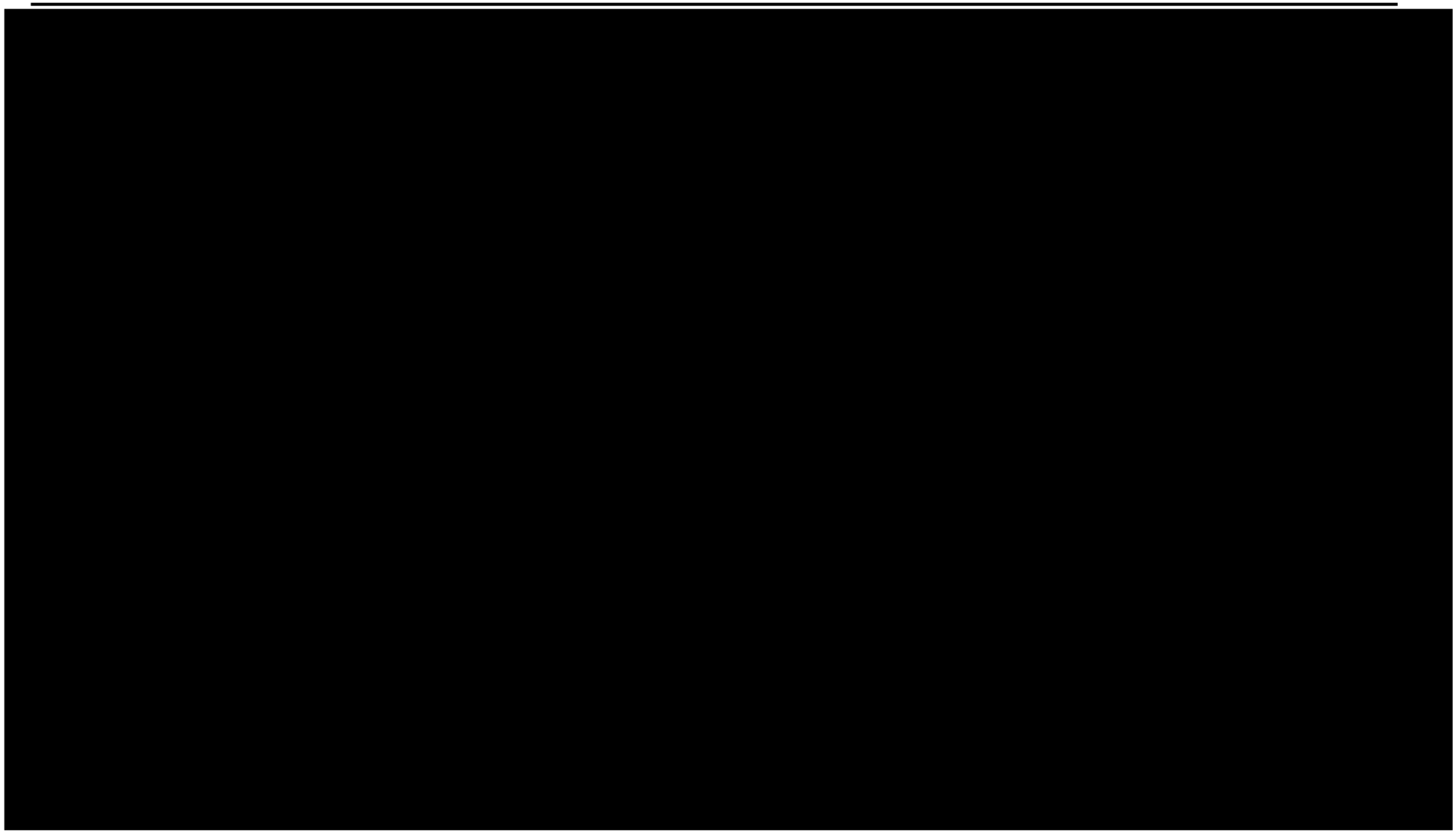
Funciones:	Recabar, registrar y revisar los datos personales en las minutas o formatos de atención a usuarios y capacitación, según correspondan con su área.
Obligaciones:	Compartir las minutas con los asistentes. Enviar a resguardo en Sistema Documental de la DGRU dichos documentos físicos o digitales. Revisar la inclusión de la información de minutas, capacitaciones y tablas de atención a usuarios en informes de rendición de cuentas de la DGRU ante otras dependencias universitarias. Realizar el proceso sin comprometer la integridad de los datos personales.
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Recabar, registrar y revisar los datos personales en las minutas o formatos de atención a usuarios y capacitación, según correspondan con su área.
Obligaciones:	Compartir las minutas con los asistentes. Enviar a resguardo en Sistema Documental de la DGRU dichos documentos físicos o digitales. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación
Funciones:	Recabar, registrar y revisar los datos personales en las minutas o formatos de atención a usuarios y capacitación, según correspondan con su área.
Obligaciones:	Compartir las minutas con los asistentes. Enviar a resguardo en Sistema Documental de la DGRU dichos documentos físicos o digitales. Realizar el proceso sin comprometer la integridad de los datos personales.

Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Rubén Ignacio Sáenz González
Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Recabar, registrar y revisar los datos personales en las minutas o formatos de atención a usuarios y capacitación, según correspondan con su área.
Obligaciones:	Compartir las minutas con los asistentes. Enviar a resguardo en Sistema Documental de la DGRU dichos documentos físicos o digitales. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Ana Laura Méndez Franco
Cargo:	Jefa de Departamento de Planeación y Seguimiento de Proyectos
Funciones:	Recabar, registrar y revisar las minutas, formatos de atención a usuario y capacitación de las coordinaciones de la DGRU.
Obligaciones:	Indicar en qué expediente de archivo se deben resguardar los documentos, enviar a resguardo en Sistema Documental de la DGRU dichos documentos físicos o digitales. Incluir la información de minutas, capacitaciones y formatos de atención a usuarios en informes de rendición de cuentas de la DGRU ante otras dependencias universitarias. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Encargado	
Nombre:	Alejandro Chávez Méndez
Cargo:	No aplica

Funciones:	Resguardar de manera segura los datos personales contenidos en los documentos físicos y digitales relacionados con minutas, capacitaciones y tablas de atención a usuarios de las plataformas digitales administradas por la DGRU.
Obligaciones:	Digitalizar los documentos que contienen los datos personales, asegurando la integridad de dichos datos personales. Archivar el documento digital en un espacio encriptado en la DGRU. Archivar el documento físico conforme a los Instrumentos de Control y Consulta Archivística de la UNAM. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Encargado	
Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica
Usuarios	
Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

5.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	DG2
Nombre del sistema DG2	Formatos de gestión interna
Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]



5.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Documentos internos generados como evidencia de reuniones, capacitaciones impartidas por el personal de la DGRU y atención a usuarios de plataformas digitales administradas por la DGRU.	Es importante para el seguimiento de los proyectos que se desarrollan en la DGRU de acuerdo con sus funciones sustantivas.	Minutas de reuniones, evidencias de capacitación y tablas de atención a usuarios de las plataformas que administra la DGRU que pueden contener información personal y laboral.
Dueño		
¿A quién pertenece el activo de información?		
Directora General		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	En el caso de los formatos de registro de atención a usuarios de las plataformas, se considerarán confidenciales toda vez que pueden incluir datos personales y únicamente personal autorizado podrá acceder a ellos.
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente manera:	Una vez ingresado el documento al Sistema Documental de la DGRU,

		no podrá ser modificado.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera:	Los documentos deben estar disponibles para que el personal autorizado de la dependencia los consulte o integre en informes institucionales.
	Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
( ) Confidencialidad	**(X) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	

5.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Formatos de gestión interna
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]

[redacted]

CONTENEDORES FÍSICOS

[redacted]

[redacted]

[redacted]

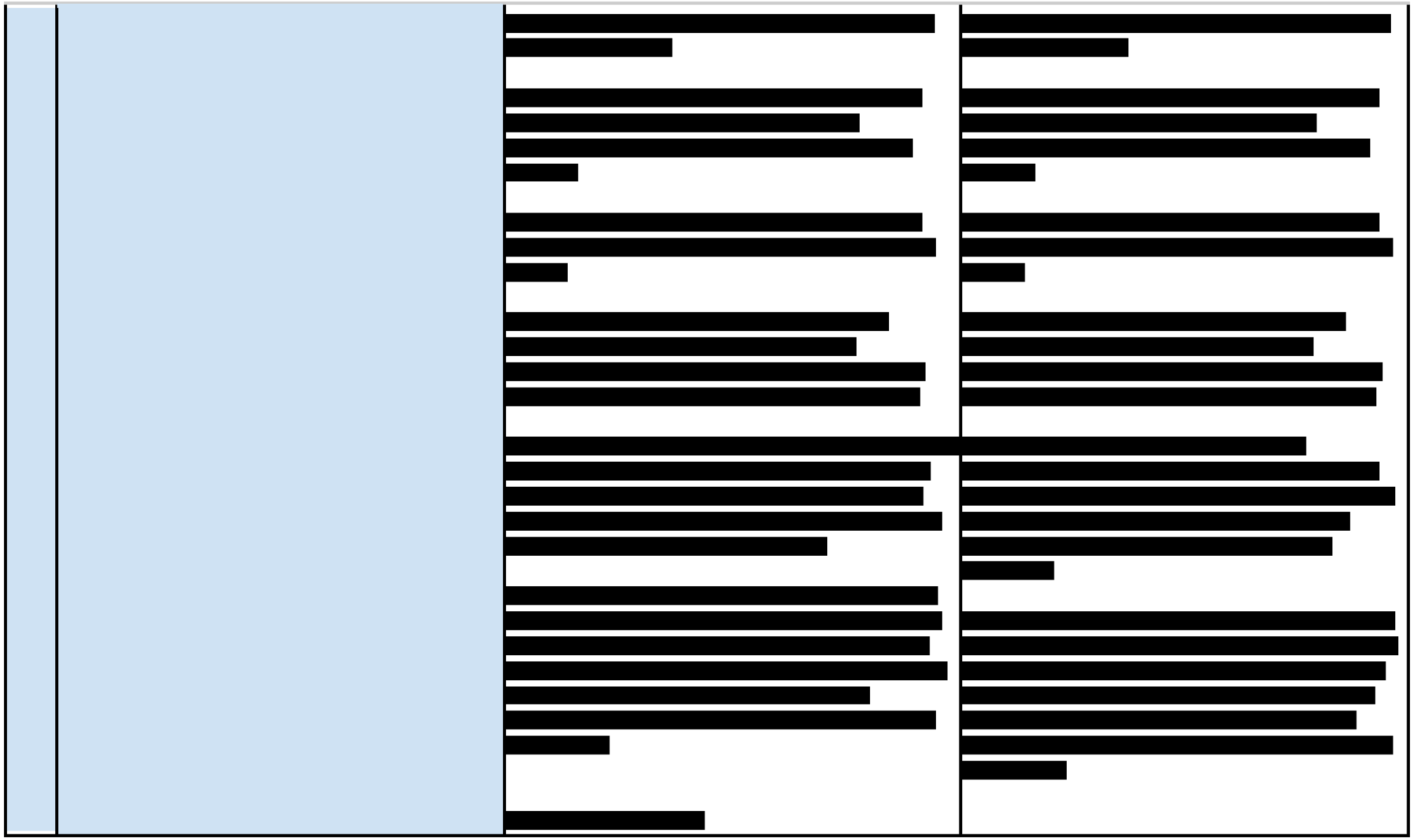
RECURSOS HUMANOS

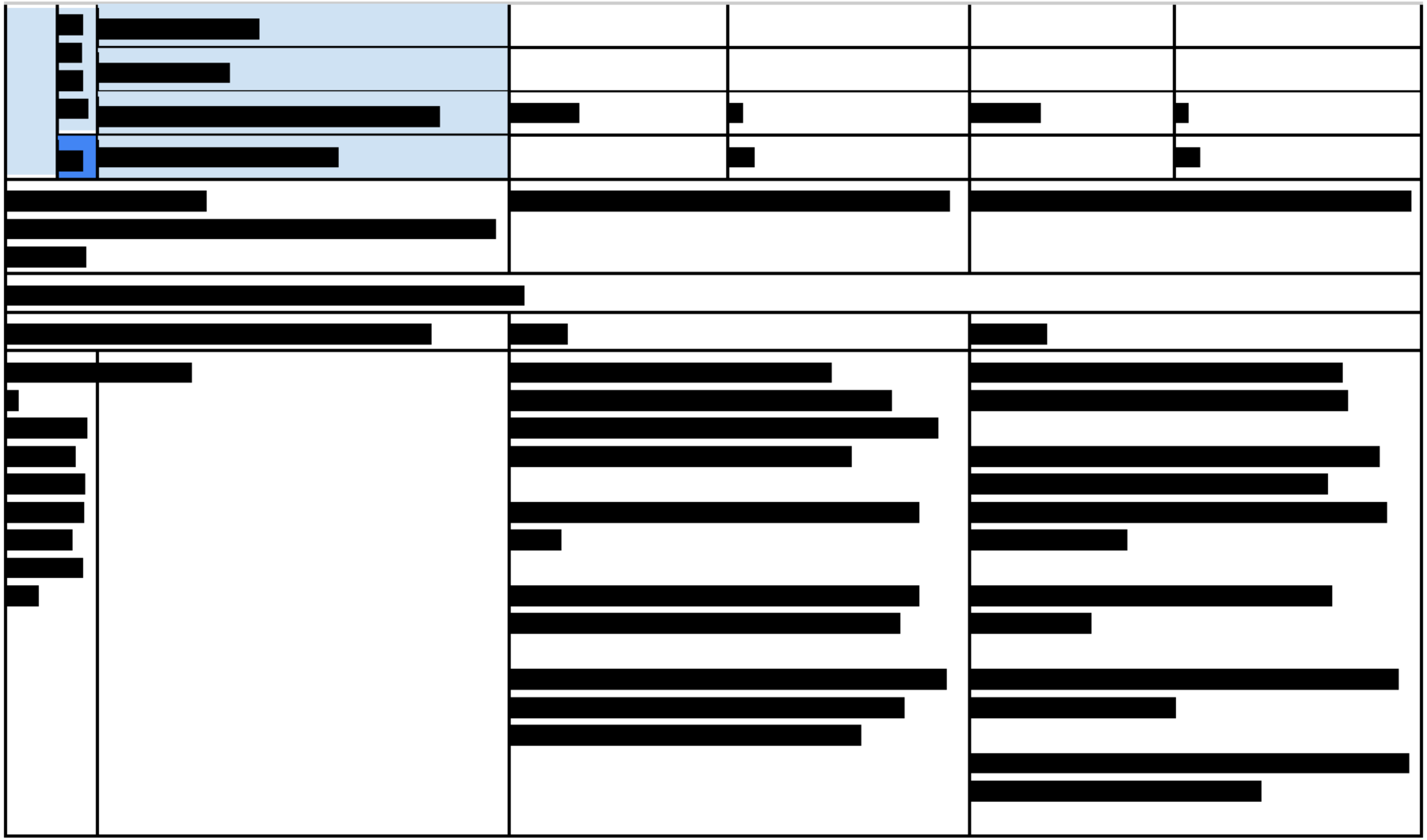
[redacted]

[redacted]

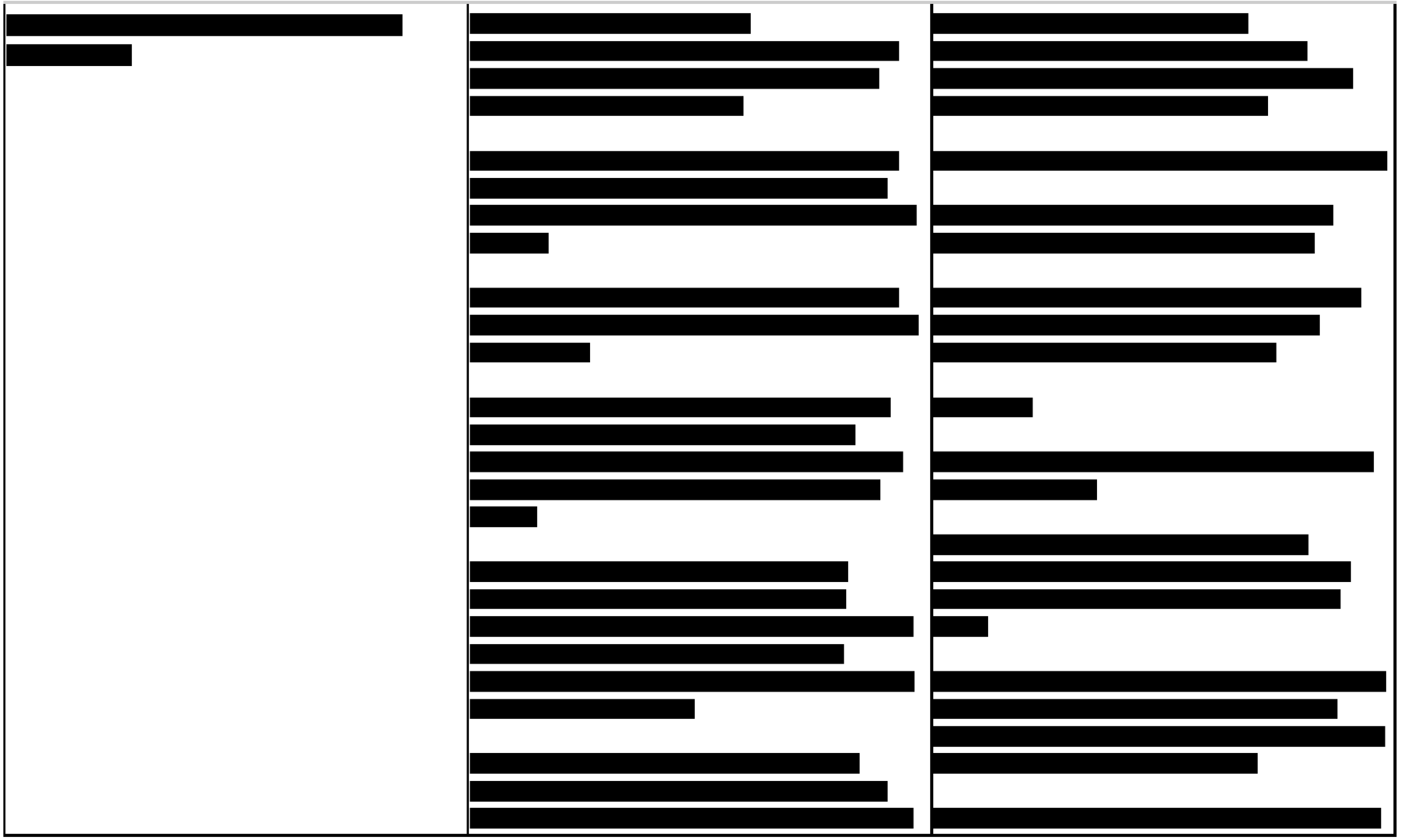
5.5. ANÁLISIS DE RIESGOS

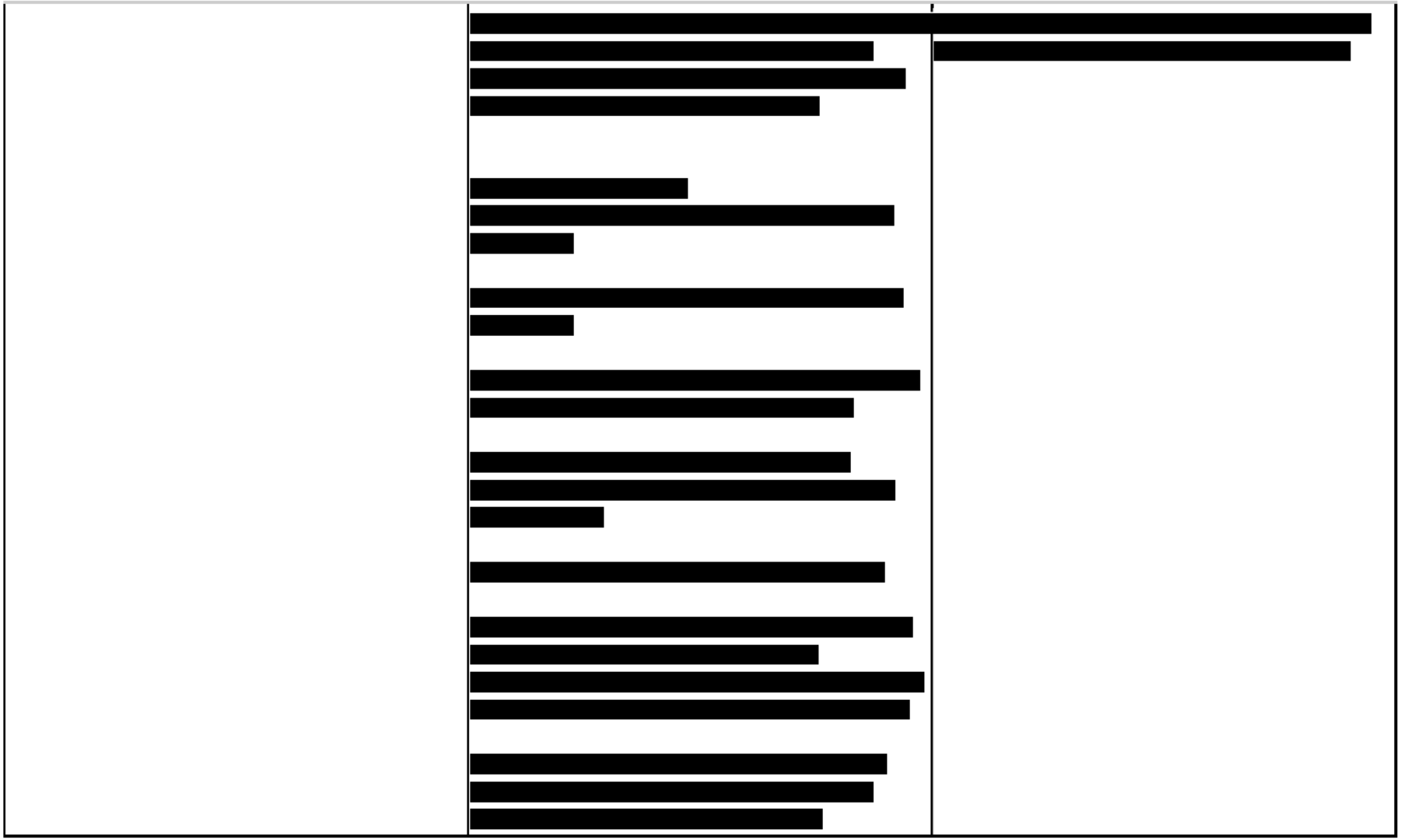
[redacted]

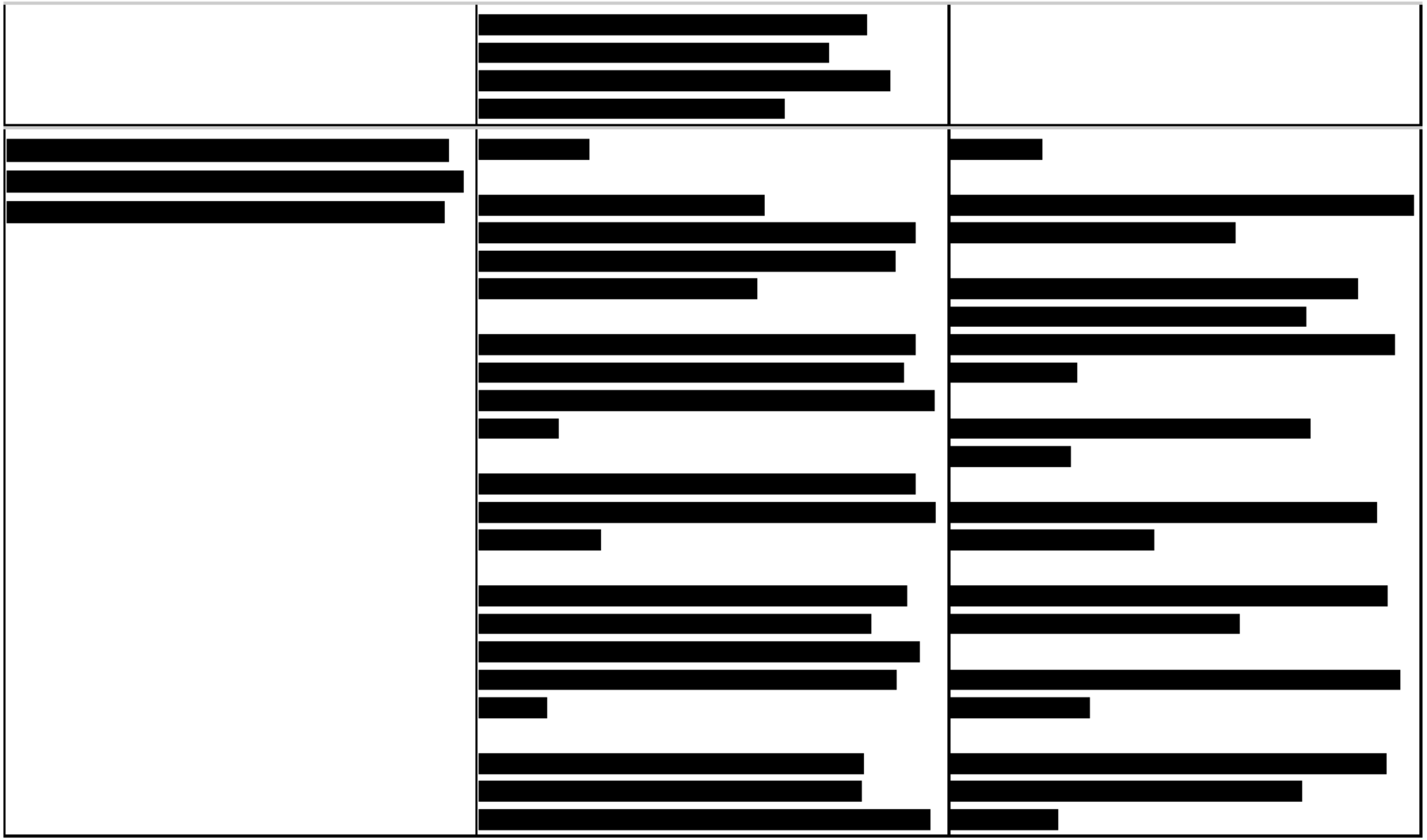


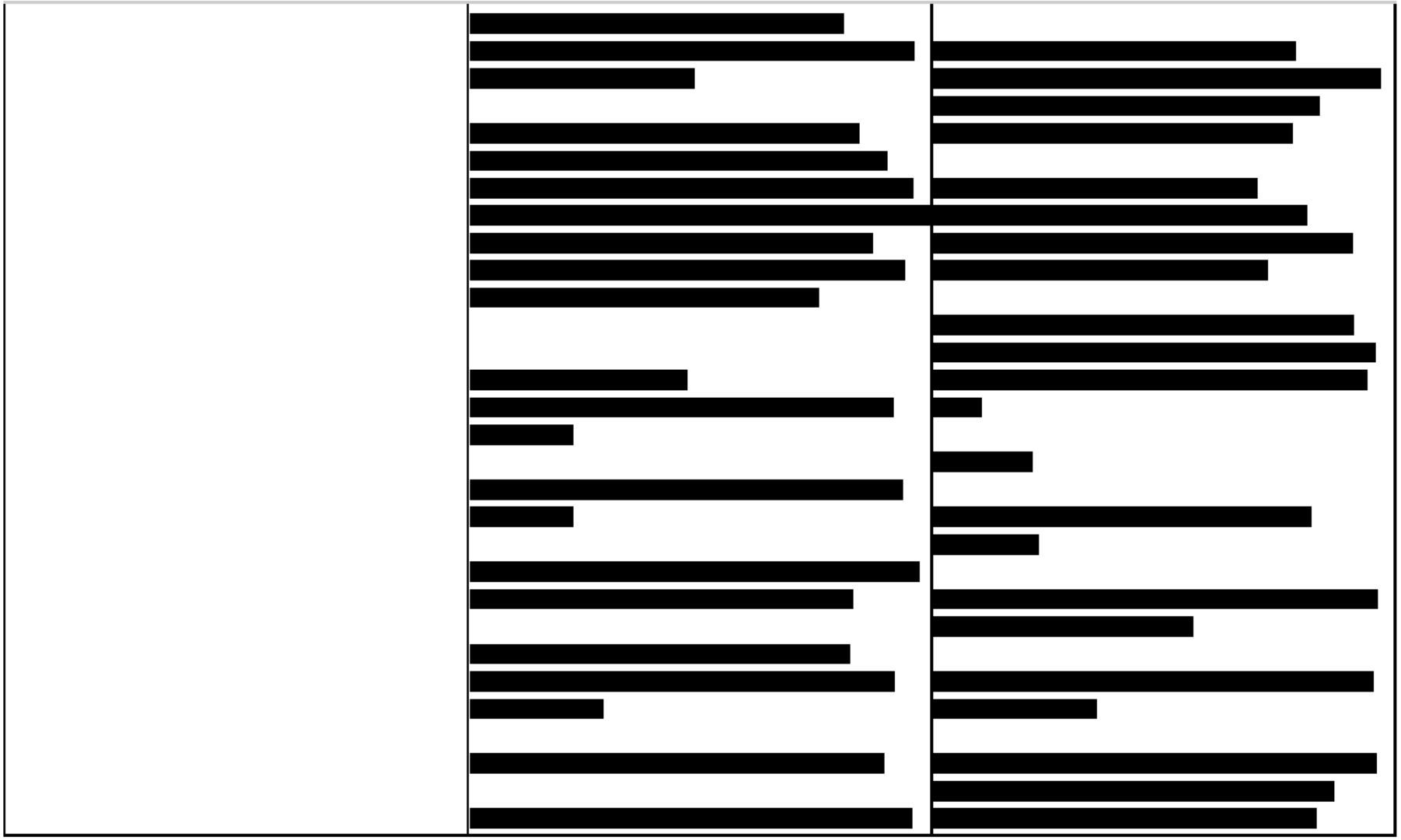


Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de Gestión Interna	
ANÁLISIS DE RIESGOS		
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]









	[redacted]	[redacted]

5.6. ANÁLISIS DE BRECHA

Dirección General, DGRU			
Identificador único	DG2		
Nombre del sistema DG2	Formatos de gestión interna		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

	[redacted]	[redacted]	[redacted]

5.7. PLAN DE TRABAJO

Dirección General, DGRU				
Identificador único	DG2			
Nombre del sistema DG2	Formatos de gestión interna			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]		[redacted]	

5.8. MEDIDAS DE SEGURIDAD

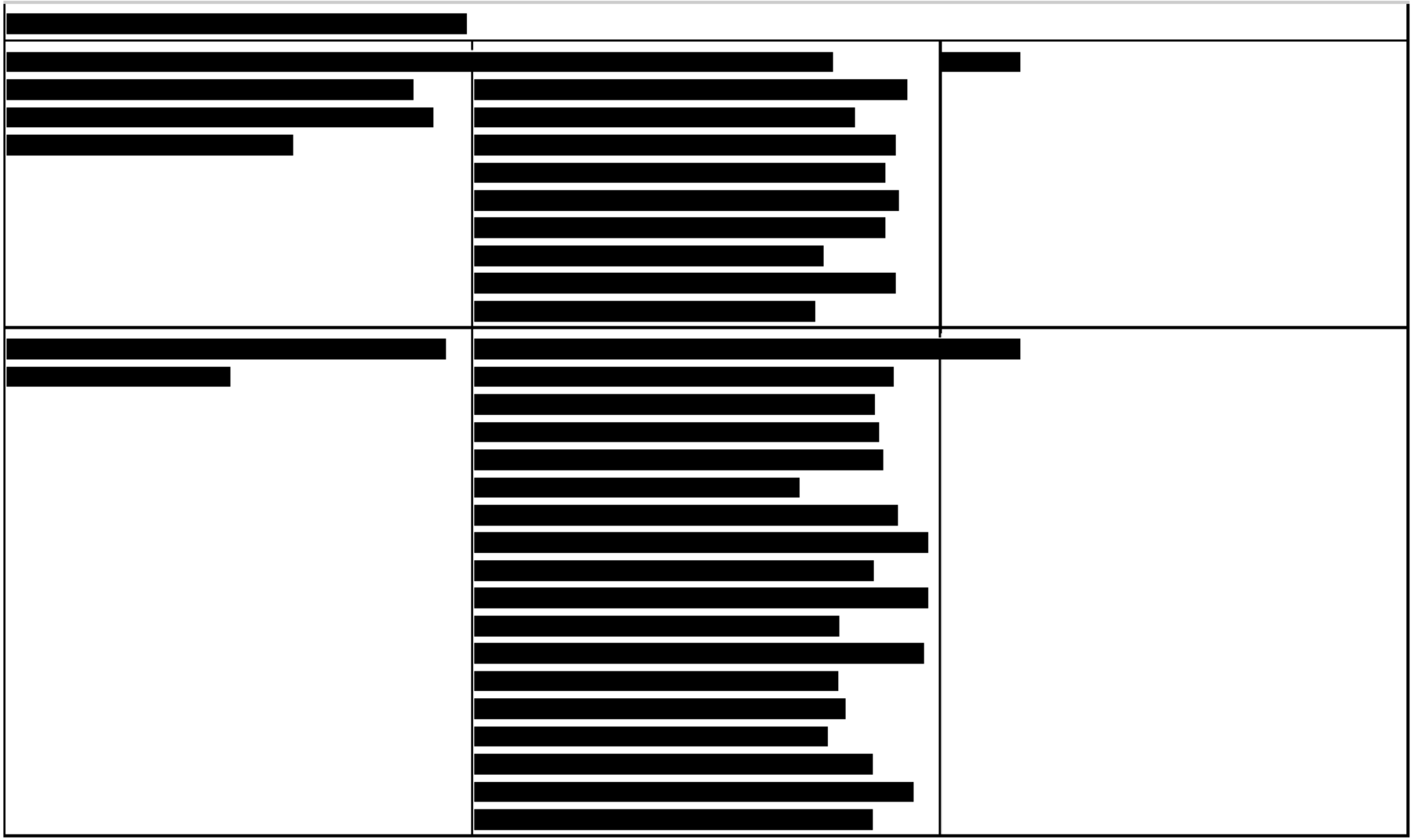
Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

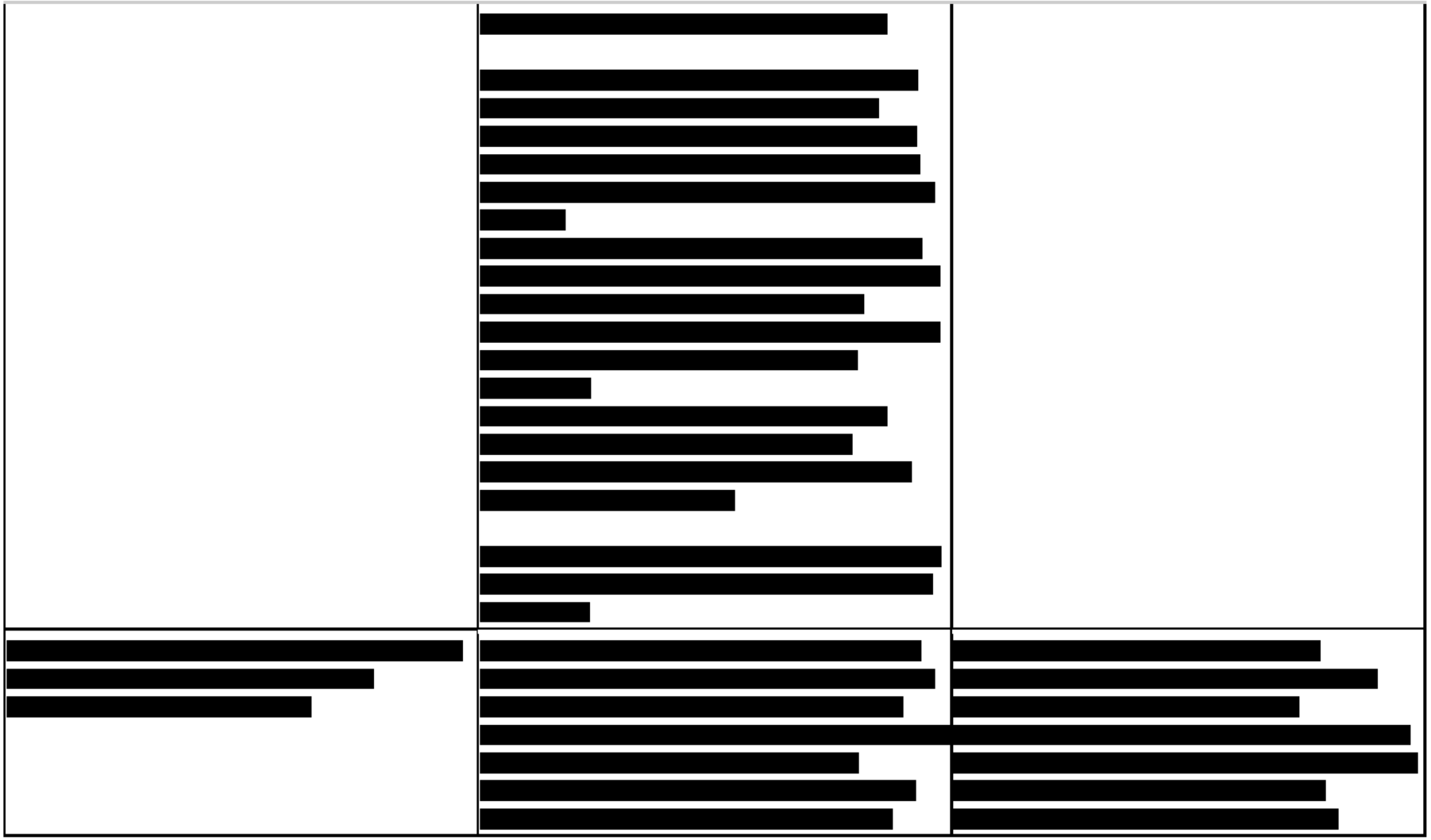
	[redacted]	

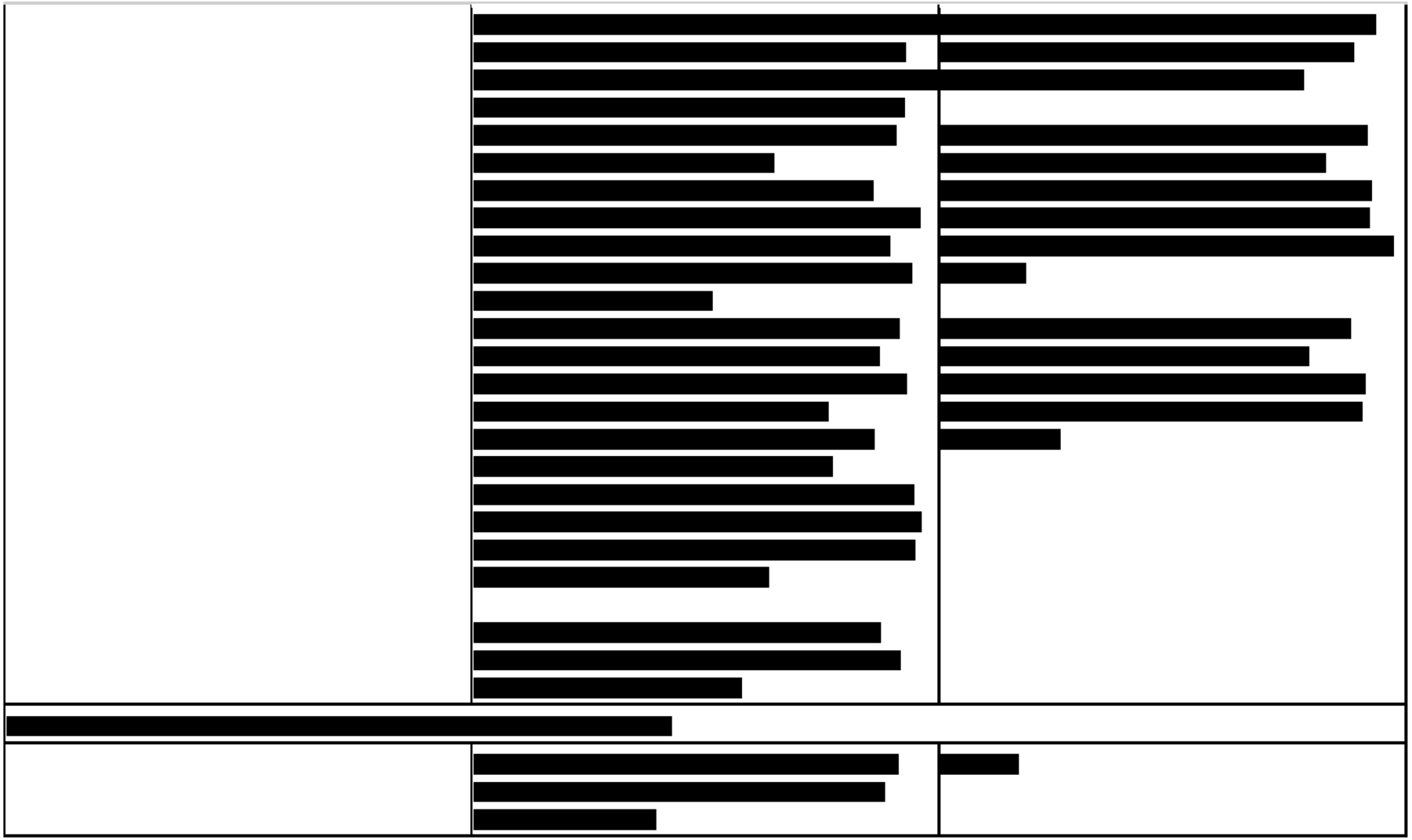
Dirección General, DGRU	
Identificador único	DG2
Nombre del sistema DG2	Formatos de gestión interna
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	

[redacted]

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**







[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Dirección General, DGRU	
Identificador único	DG2
Nombre del sistema DG2	Formatos de gestión interna

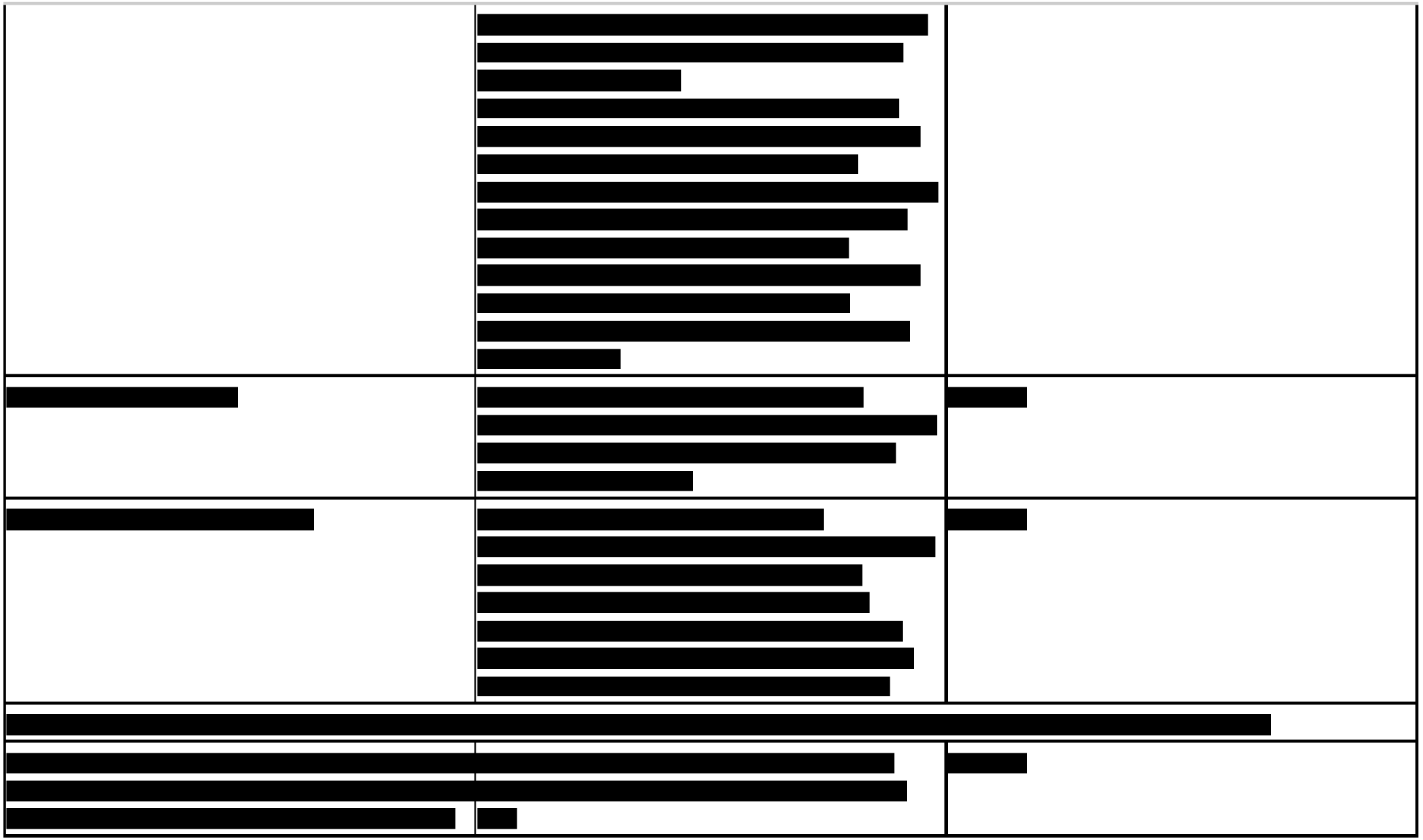
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]

		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

[redacted]		
	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]

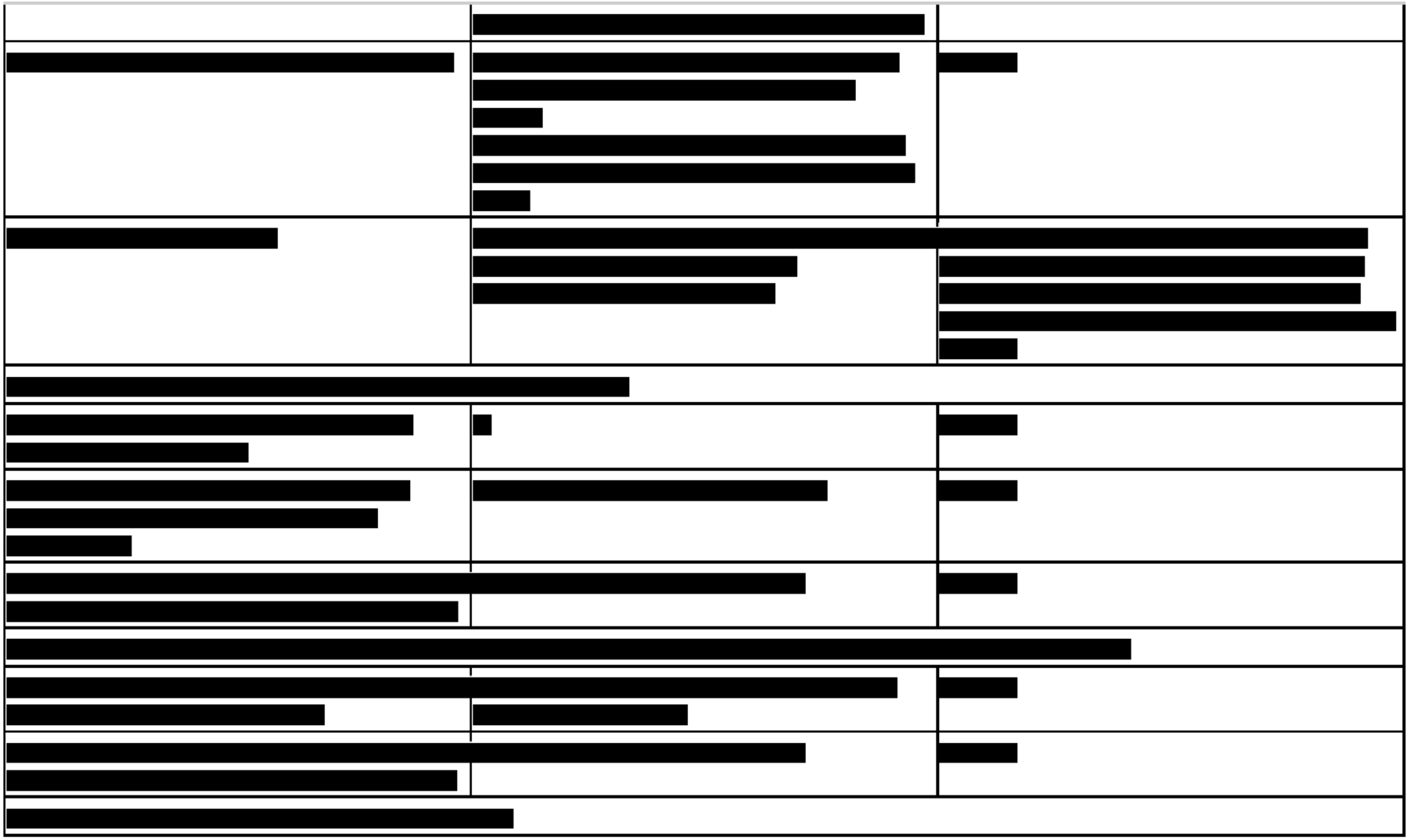


[redacted]	[redacted]	
[redacted]		
[redacted]	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

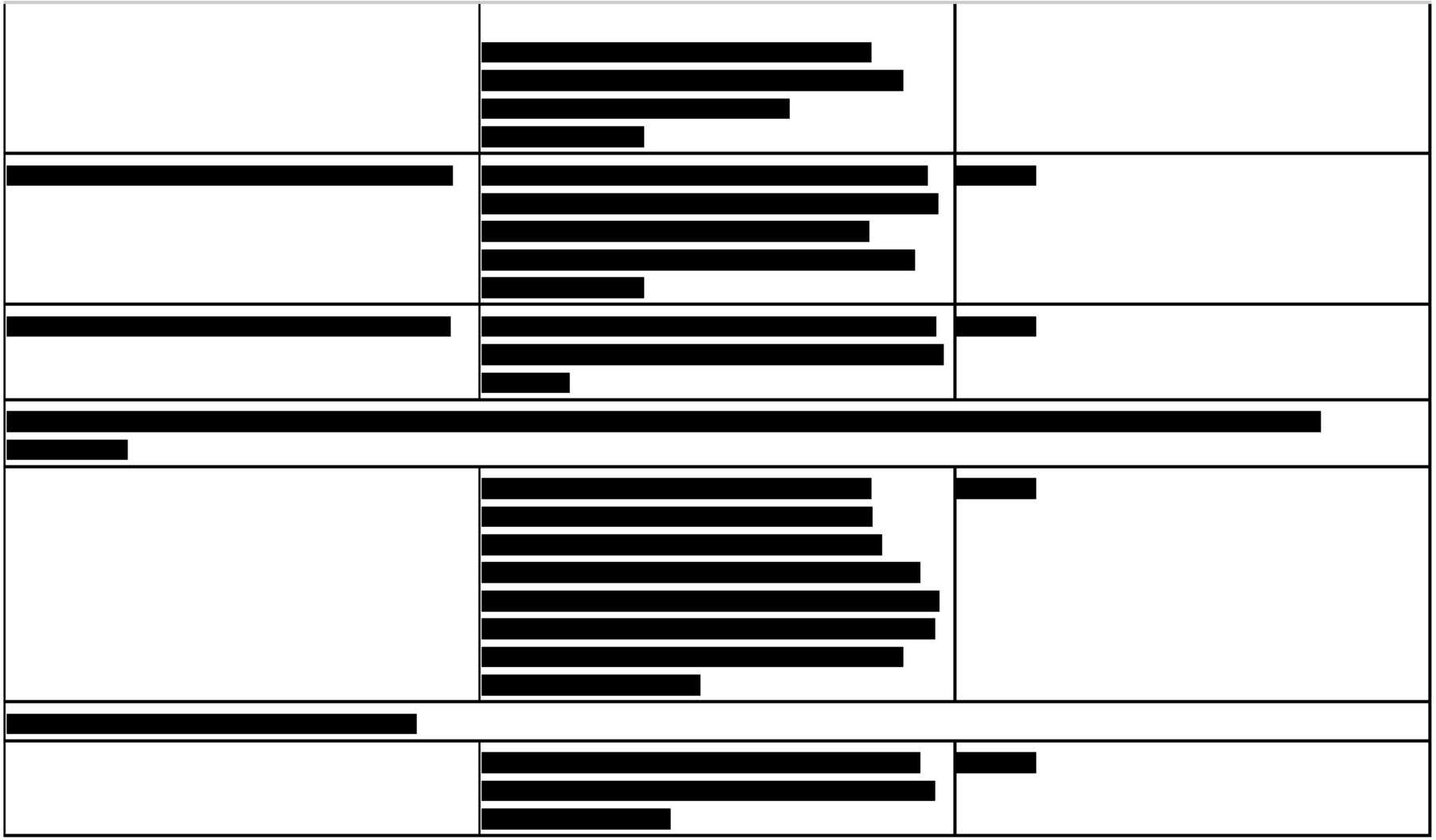
[redacted]		[redacted]

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		
[redacted]		

Dirección General, DGRU	
Identificador único	DG2
Nombre del sistema DG2	Formatos de gestión interna
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	
[redacted]	
[redacted]	



[redacted]		
	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

5.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General, DGRU	
Identificador único	DG2
Nombre del sistema DG2	Formatos de gestión interna

Medida de seguridad	Resultado de evaluación	Responsable
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Dirección General, DGRU		
Identificador único	DG2	
Nombre del sistema DG2	Formatos de gestión interna	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

5.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU				
Identificador único	DG2			
Nombre del sistema DG2	Formatos de gestión interna			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos	Monitorear la publicación de normatividad o información relevante en materia de datos personales para	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

personales.	revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.			

Programa de difusión de la protección a los datos personales

Dirección General, DGRU				
Identificador único	DG2			
Nombre del sistema DG2	Formatos de gestión interna			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales. - Procedimientos de borrado seguro de correos electrónicos y de archivos.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones de Colecciones y Datos de Investigación, Sistema de Repositorios Universitarios, Desarrollo Tecnológico e Infraestructura y de Planeación, Gestión y Normatividad involucrado con el tratamiento de datos personales. Frecuencia de la actualización una vez al año o antes si se considera necesario.	Alta

- Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.				

Anexo 6. DG3 Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos

6.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: Nombre, domicilio, correo electrónico, firma, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, fotografía, idioma o lengua. 1b. Datos laborales: Institución, nombramiento, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales. 1c. Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. 1d. Características físicas: Color de piel, ojos y cabello, señas particulares, complexión, discapacidades, entre otros. 2. Datos personales sensibles: Opiniones políticas, origen racial o étnico, creencias religiosas, creencias filosóficas y morales, afiliación sindical, estado de salud presente o futuro (historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis.
¿Cómo se obtienen los datos personales?	Físico (X) Digital (X)
¿Para qué se usan?	Los datos personales incluidos en el formato de autorización para el uso de imagen o voz personales y contenidos, se utilizan para contactar a las personas asistentes a los eventos. El formato solicita incluir fotocopia o imagen de identificación oficial. Los datos personales incluidos en la identificación oficial se usan para reconocer a la persona

	titular de los derechos y obtener la autorización para el uso de imagen y/o voz, a través del correspondiente formato. Puede haber datos personales que se expresan durante el evento que se está grabando. Dichas grabaciones se usan con fines académicos, informativos y de difusión.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal (X)	Gobierno Estatal (X) Gobierno Municipal (X) Personas físicas (X) Personas morales (X) Áreas Universitarias (X) La fotocopia o imagen de la identificación oficial y el formato de autorización para el uso de imagen y/o voz requisitado, no se comparten. Los datos personales incluidos en las grabaciones de voz y/o imagen se pueden compartir con los asistentes al evento, en cuyo caso podría ser personal interno o externo a la Universidad. Se pueden compartir con otras áreas universitarias a las que se rinde cuenta de las Actividades que realiza la DGRU o se pueden publicar y difundir en diferentes medios electrónicos o plataformas digitales.
¿Dónde se alojan?	[redacted]o	

	[redacted]
¿Cuánto tiempo se da tratamiento?	La disposición de los documentos y grabaciones es el establecido en los Instrumentos de Control y Consulta Archivística de la UNAM vigentes.
Responsable	
Nombre:	Tila María Pérez Ortiz
Cargo:	Directora General de Repositorios Universitarios
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen y/o voz, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen y/o voz requisitado, así

	como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen y/o voz, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización

	para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Rubén Ignacio Sáenz González
Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Ana Laura Méndez Franco

Cargo:	Jefa de Departamento de Planeación y Seguimiento de Proyectos
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Responsable	
Nombre:	Edurne Dolores Uriarte Santillán
Cargo:	Jefa de Departamento de Inventario de Colecciones y Datos de Investigación
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Responsable	
Nombre:	Daniel Pérez Castillo
Cargo:	Jefe de Departamento de Datos de Investigación
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Responsable	
Nombre:	Roberto Rico Chávez
Cargo:	Jefe de Departamento de Infraestructura, Centro de Datos y Servicios
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión.

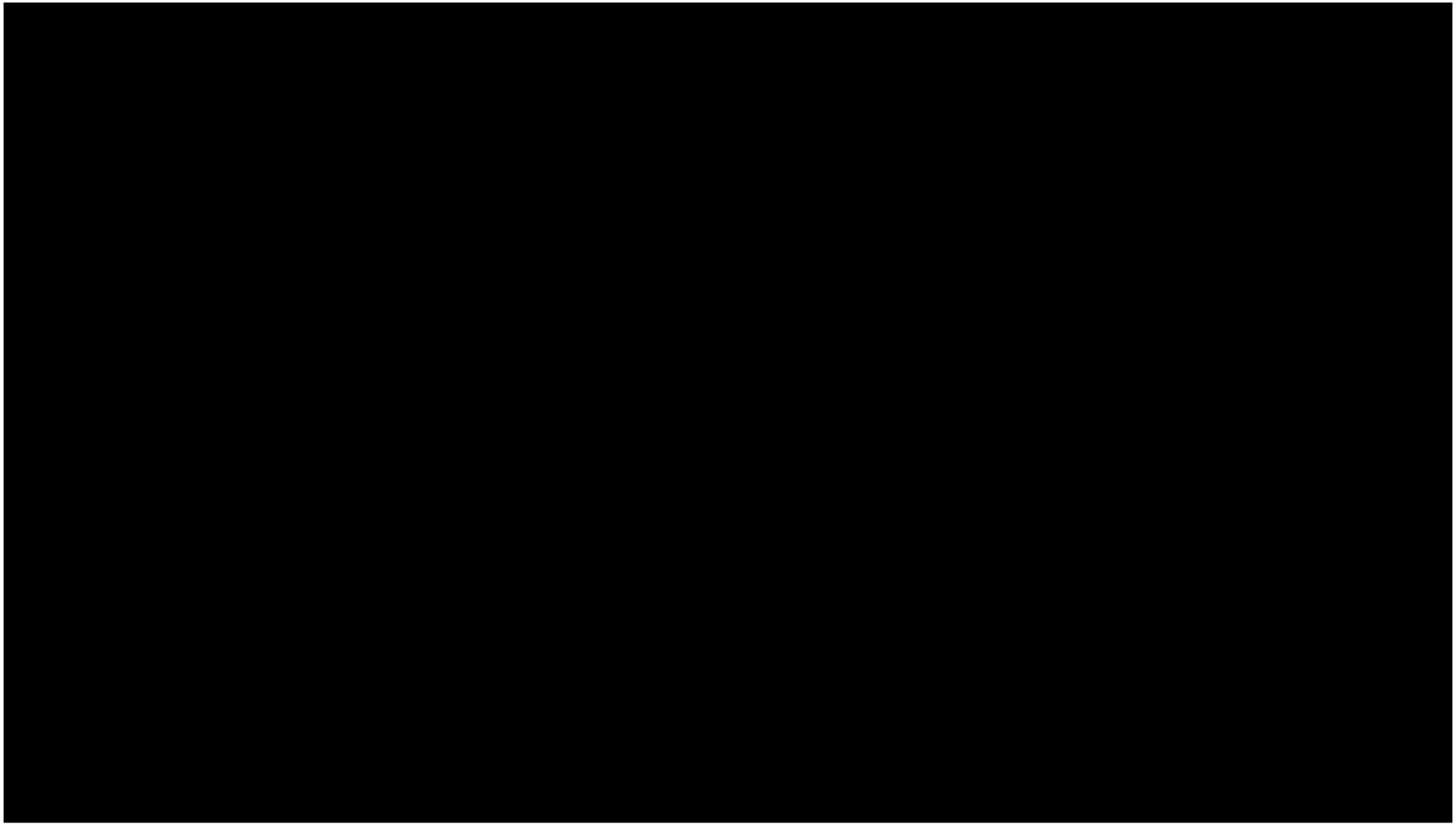
	Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Responsable	
Nombre:	Oscar Hernández Hernández
Cargo:	Jefe de Departamento de Instalación y Soporte de Repositorios Universitarios
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Responsable	
Nombre:	Areli Plancarte Salas
Cargo:	Asistente Ejecutivo
Funciones:	Recabar, registrar y revisar los datos personales solicitados en los formatos de autorización para el uso de imagen o voz personales y contenidos.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado, así como la grabación. Revisar la inclusión de la grabación de imagen o voz personales y contenidos en informes de

	rendición cuentas de la DGRU ante otras dependencias universitarias. En caso de que aplique, compartir la grabación de imagen o voz personales y contenidos, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	Alejandro Chávez Méndez
Cargo:	No aplica
Funciones:	Resguardar de manera segura los datos personales contenidos en los formatos de autorización para el uso de imagen o voz personales y contenidos, así como las grabaciones relacionadas con los eventos organizados por la DGRU.
Obligaciones:	Digitalizar los formatos de autorización para el uso de imagen o voz personales y contenidos y la identificación oficial que contienen los datos personales, asegurando la integridad de dichos datos personales. Archivar los formatos de autorización para el uso de imagen o voz personales y contenidos, la fotocopia o imagen de la identificación oficial y las grabaciones en un espacio encriptado en la DGRU. Archivar los formatos de autorización para el uso de imagen o voz personales y contenidos, y la fotocopia o imagen de la identificación oficial y las grabaciones conforme a los Instrumentos de Control y Consulta Archivística de la UNAM. En caso de que sea indicado por la persona que lo supervisa o la directora general, compartir la grabación de imagen y/o voz, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Encargado	
Nombre:	Personal de servicios profesionales

Cargo:	No aplica
Funciones:	Recabar, registrar y revisar los datos personales de los asistentes a los eventos organizados por la DGRU y formato de autorización para el uso de imagen y/o voz requisitado, así como la grabación, según corresponda a la tarea encomendada por el personal que lo supervisa.
Obligaciones:	Enviar a resguardo en Sistema Documental de la DGRU, la fotocopia o imagen de la identificación oficial, formatos de autorización para el uso de imagen o voz personales y contenidos, requisitado, así como la grabación. En caso de que sea indicado por la persona que lo supervisa, compartir la grabación de imagen y/o voz, para fines académicos, informativos y de difusión. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Persona a cargo de la coordinación en que colabore y Dirección General
Usuarios	
Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

6.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]



6.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Fotocopia o imagen de la identificación oficial, formato de autorización para el uso de imagen o voz personales y contenidos requisitado y grabación.	Es importante para la identificación y acopio de permisos de uso de imagen y/o voz en materiales que se generan en el marco de las colaboración de DGRU con diferentes entidades o dependencias internas o externas a la Universidad.	Son formatos de autorización para el uso de imagen o voz personales y contenidos requisitado, fotocopia o imagen de identificación oficial y grabaciones de imagen y/o voz que contienen datos personales relacionados con los asistentes a eventos organizados por la DGRU.
Dueño		
¿A quién pertenece el activo de información?		
Directora General		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	En el caso de los formatos de autorización para el uso de imagen o voz personales y contenidos, y la fotocopia o imagen de identificación oficial, se considerarán confidenciales toda vez que incluyen datos personales y únicamente personal autorizado

		podrá acceder a ellos. Las grabaciones pueden ser compartidas con personas internas o externas a la Universidad, con fines académicos, informativos y de difusión.
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente manera:	Una vez recabada la información, no podrá ser modificada.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera: Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	Los formatos de autorización para el uso de imagen o voz personales y contenidos, y la fotocopia o imagen de identificación oficial son de acceso restringido. Las grabaciones deben estar disponibles para que el personal autorizado de la dependencia los consulte o integre en informes institucionales. Las grabaciones pueden estar disponibles para personas internas o externas a la Universidad, con fines académicos, informativos o de difusión.
( ) Otro		

Requisitos de seguridad más importante

¿Cuál es el requisito de seguridad más importante para este activo?			
(X) Confidencialidad	**( ) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	

DESCRIPCIÓN DE CONTENEDOR	DUEÑO(S)
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]

[redacted]	
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	

6.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]		[redacted]	[redacted]

[redacted]					
[redacted]					
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
[redacted]				[redacted]	
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
[redacted]				[redacted]	[redacted]
[redacted]				[redacted]	
[redacted]			[redacted]	[redacted]	[redacted]
[redacted]			[redacted]	[redacted]	[redacted]

CONTENEDORES FÍSICOS

[redacted]			
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]			
[redacted]		[redacted]	[redacted]

[redacted]			
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]			
[redacted]		[redacted]	[redacted]

[redacted]

[redacted]					
[redacted]					
[redacted]					

RECURSOS HUMANOS

[redacted]

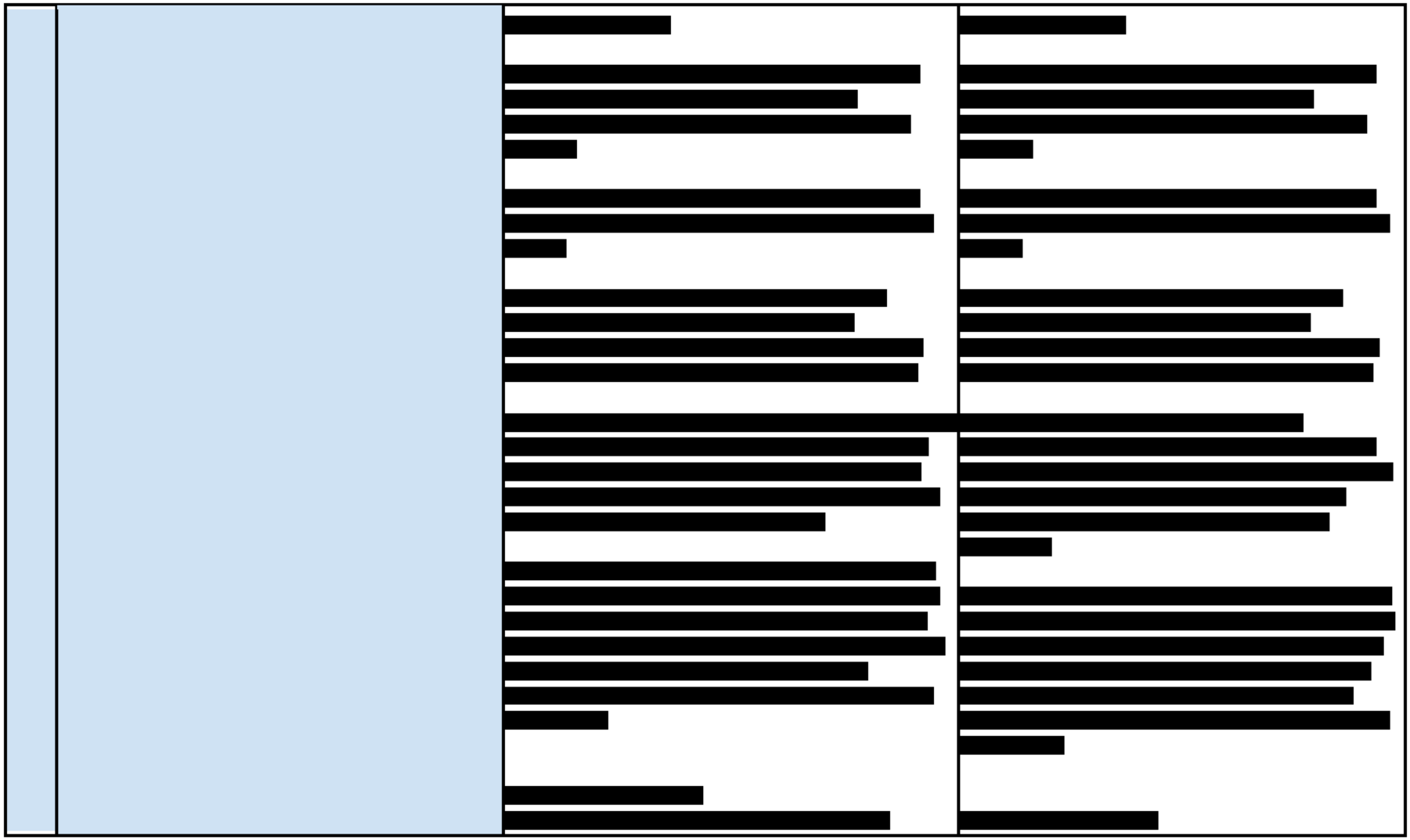
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

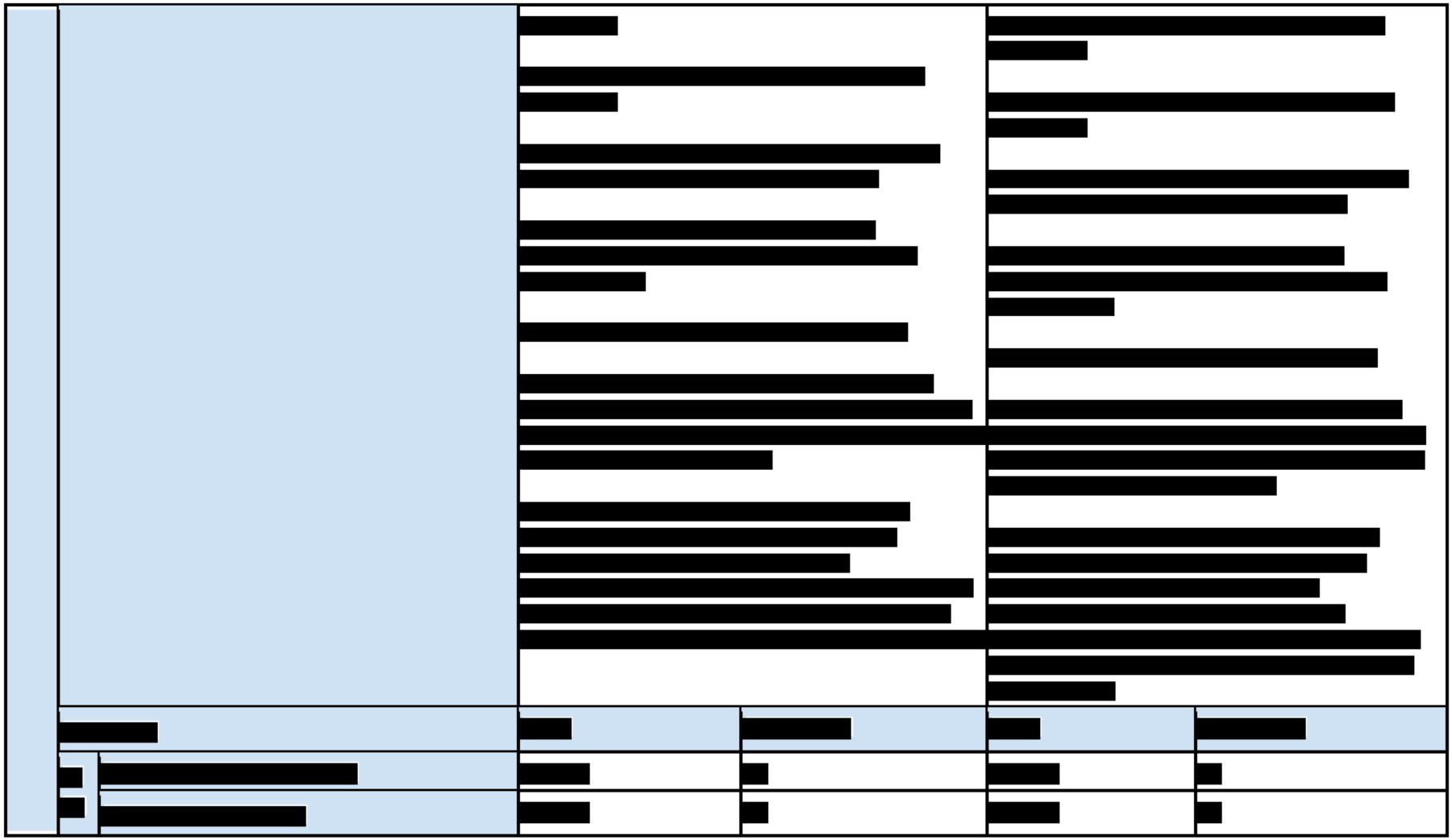
[redacted]			

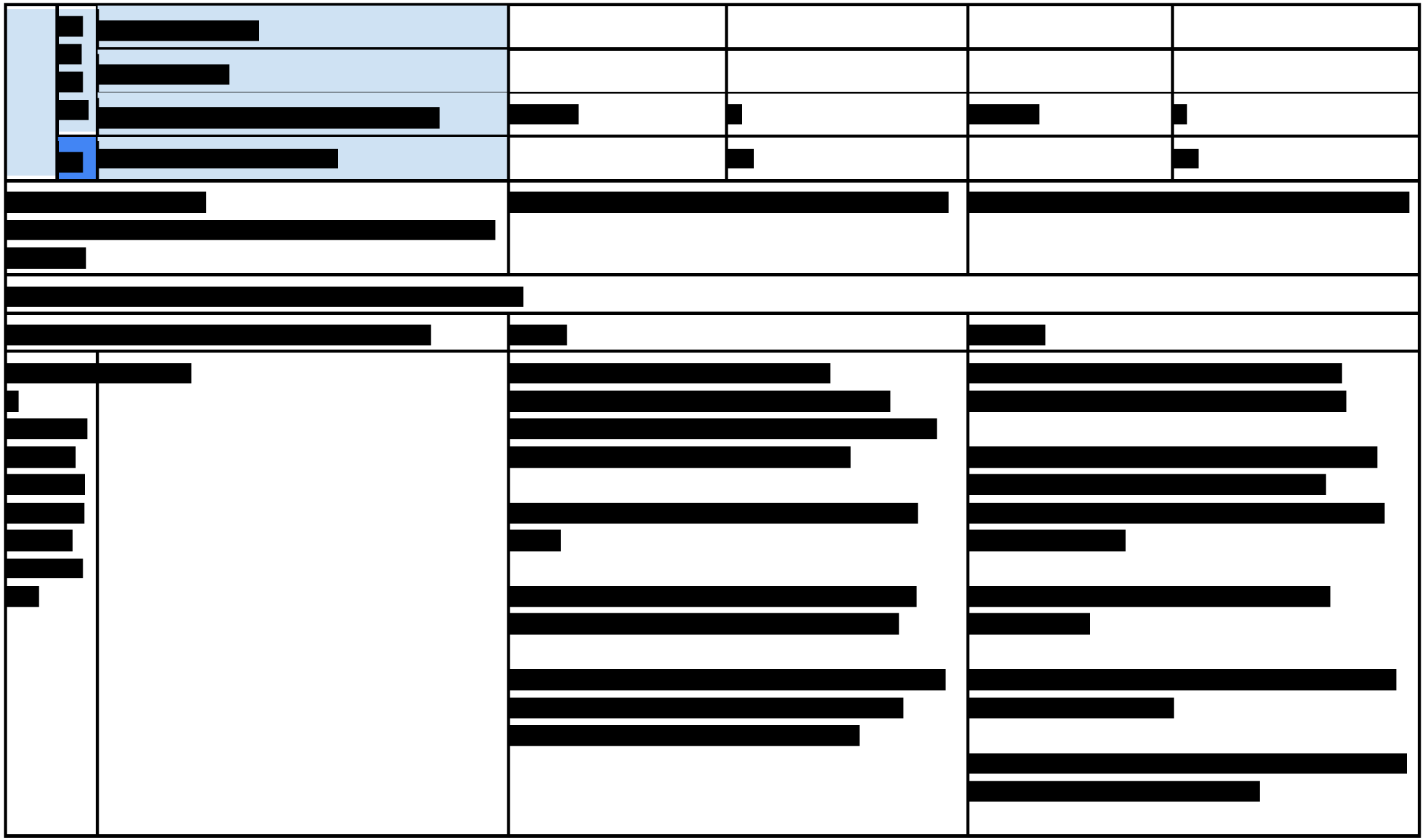
Escenario 2: **Situación en la que una persona externa a la DGRU puede acceder a los activos de información y podría (accidental o intencionadamente) permitir que él activo pueda ser:**			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

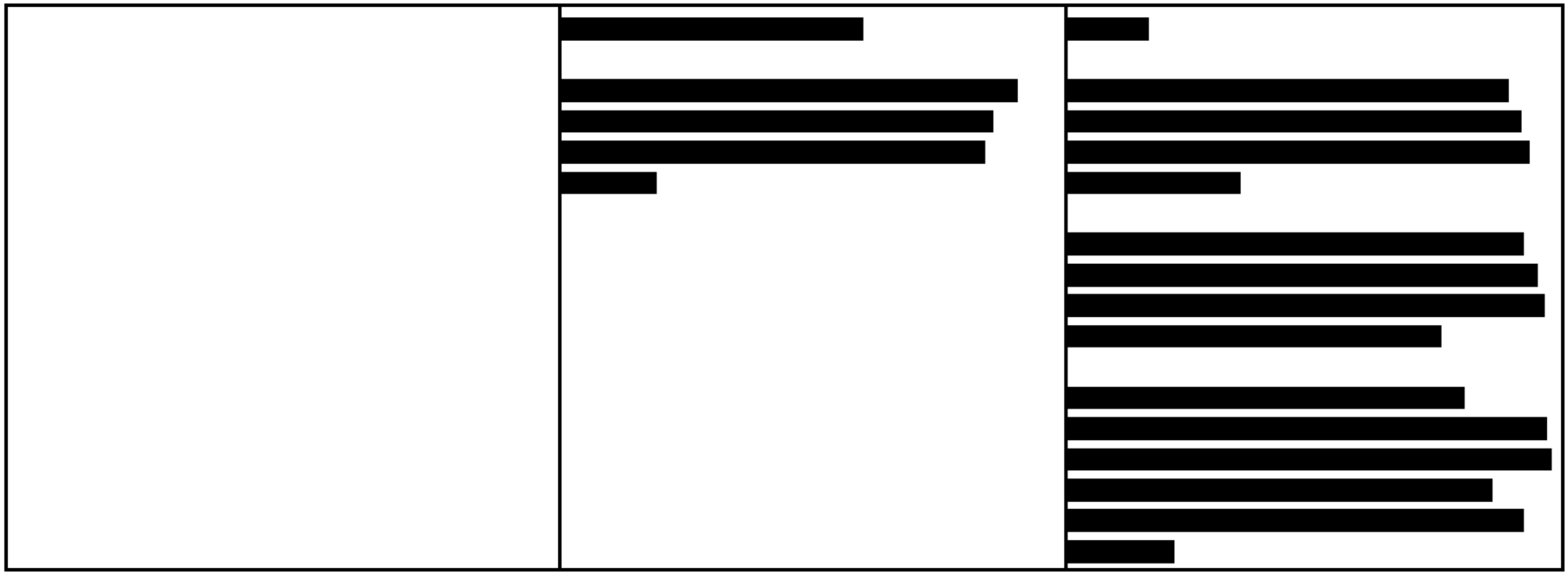
6.5. ANÁLISIS DE RIESGOS

[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]





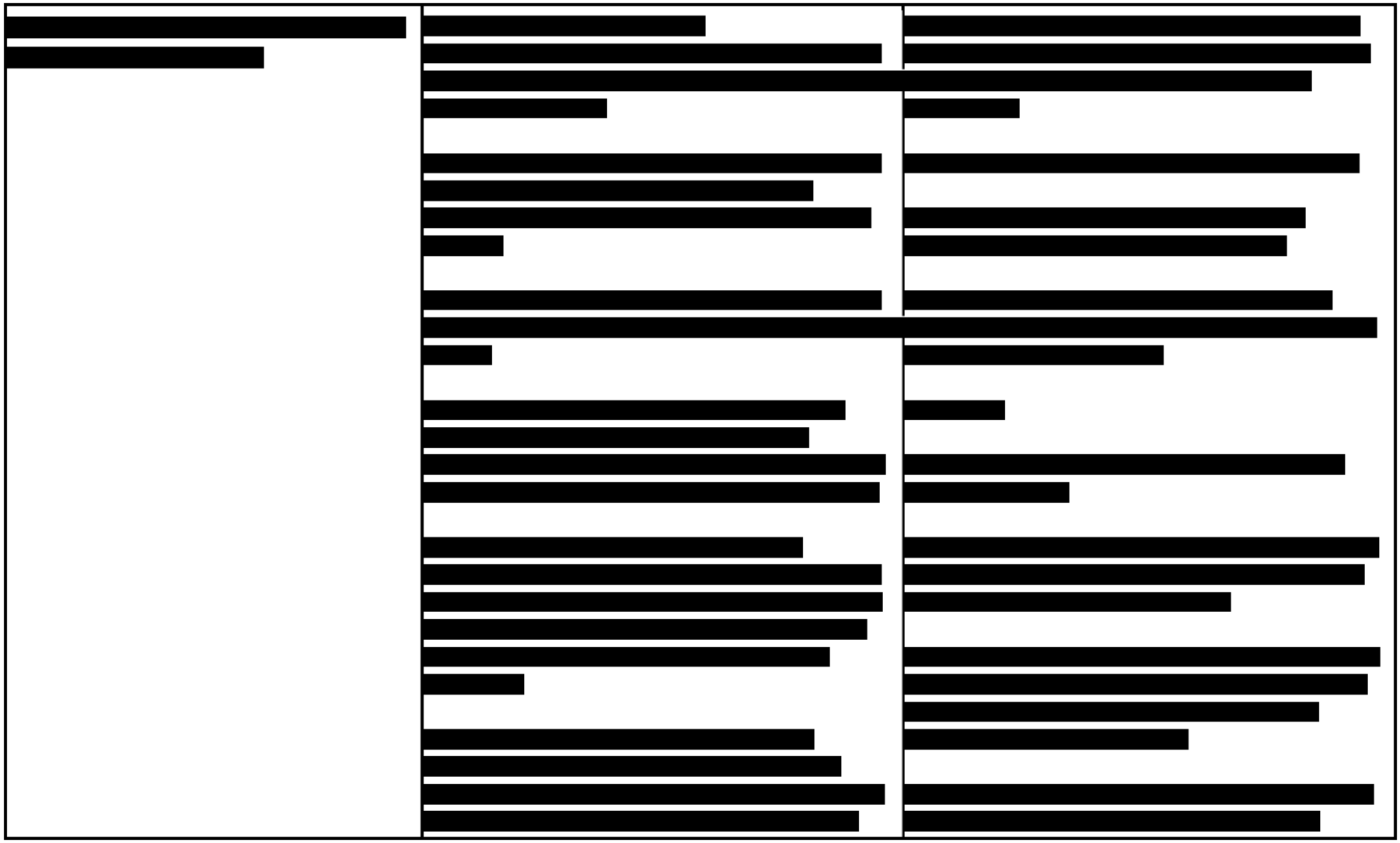


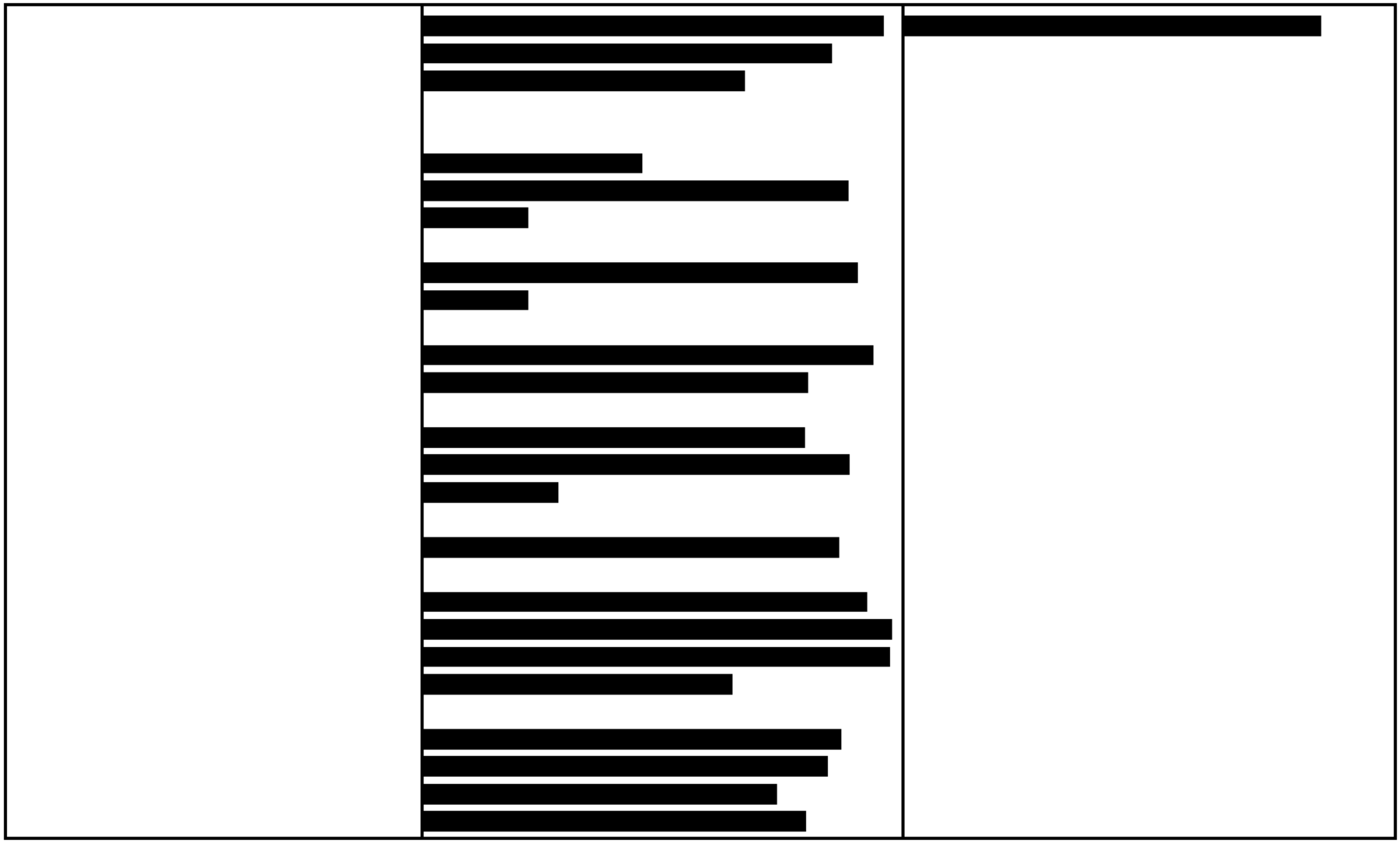


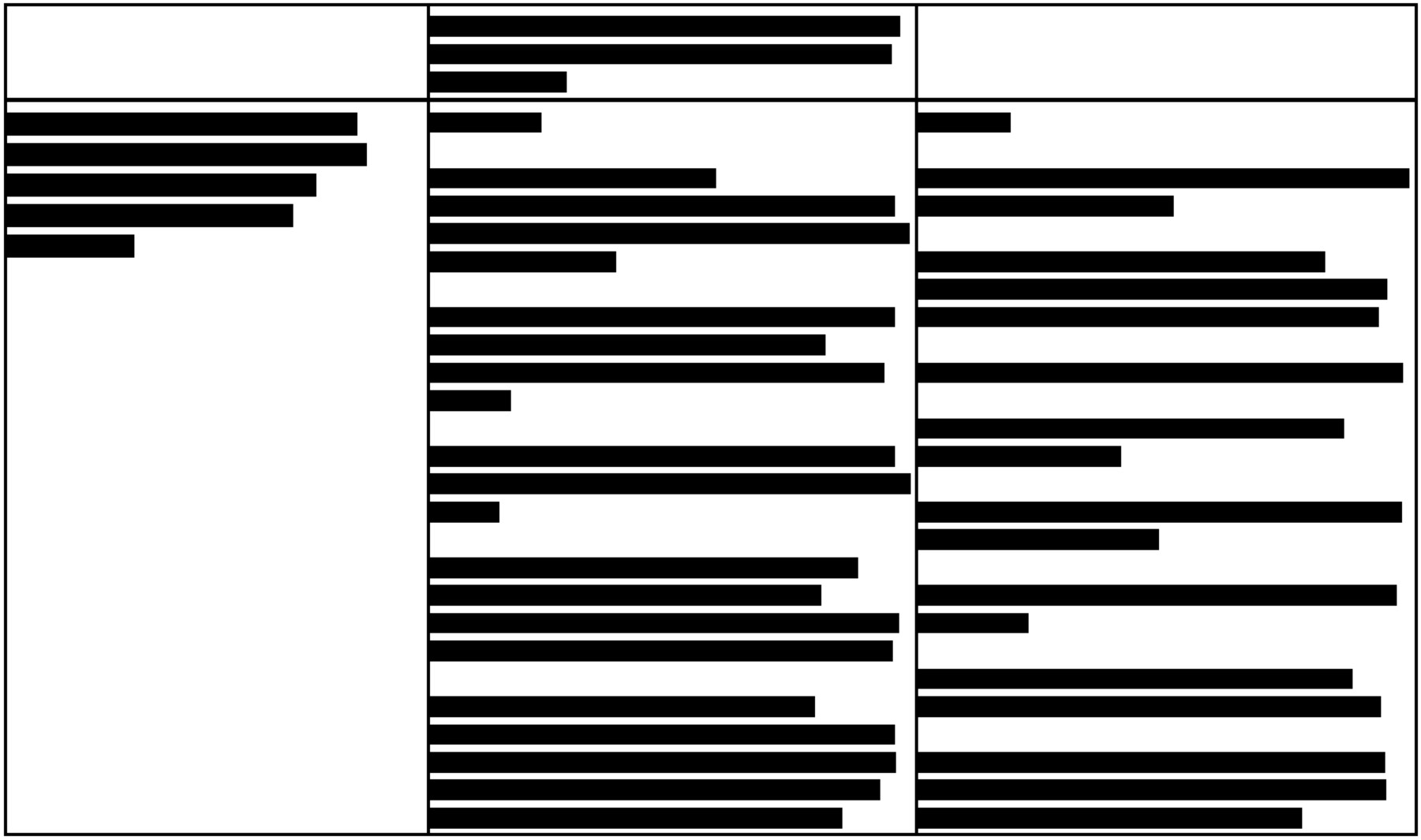
Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos

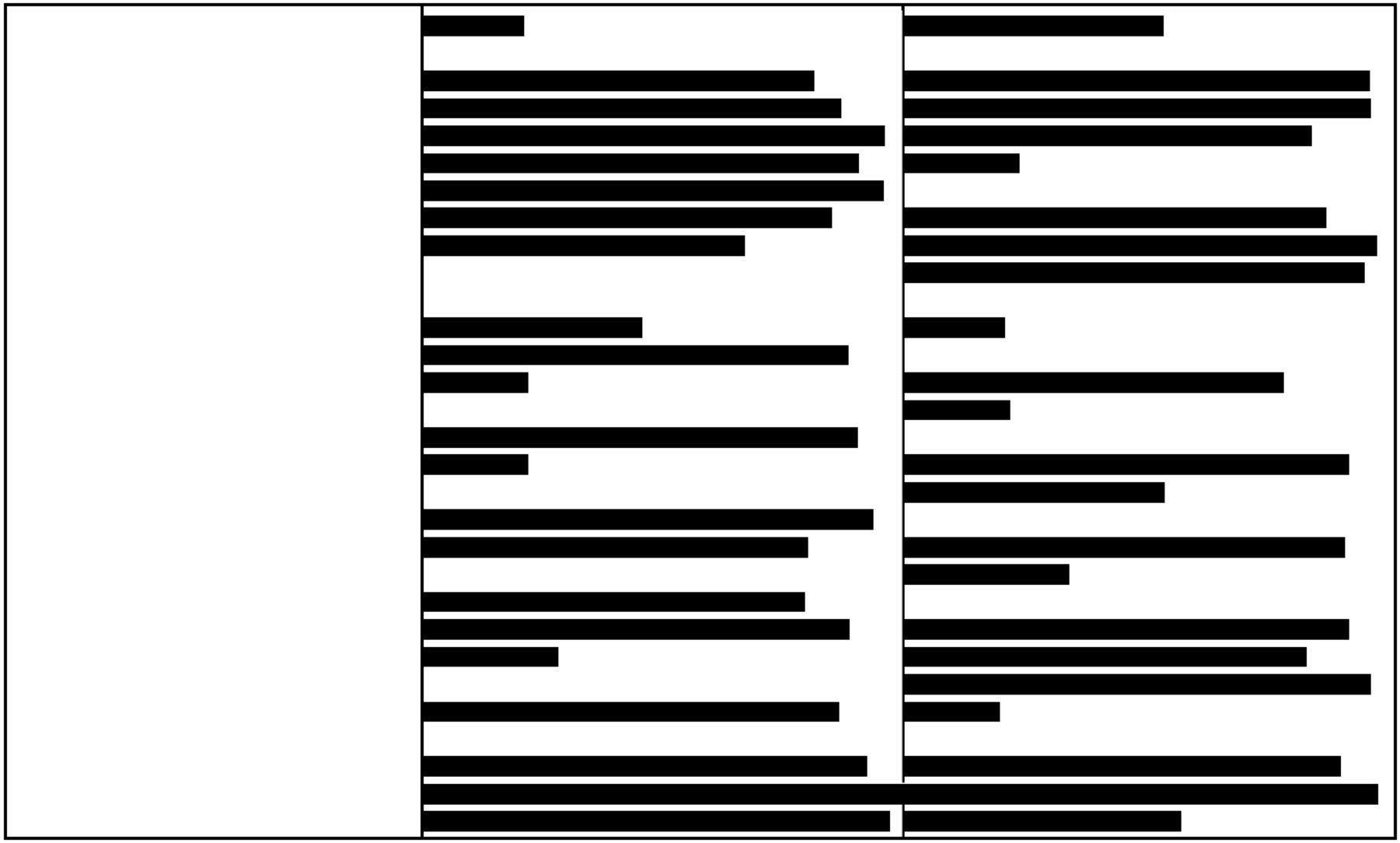
ANÁLISIS DE RIESGOS

Riesgo	Impacto	Mitigación







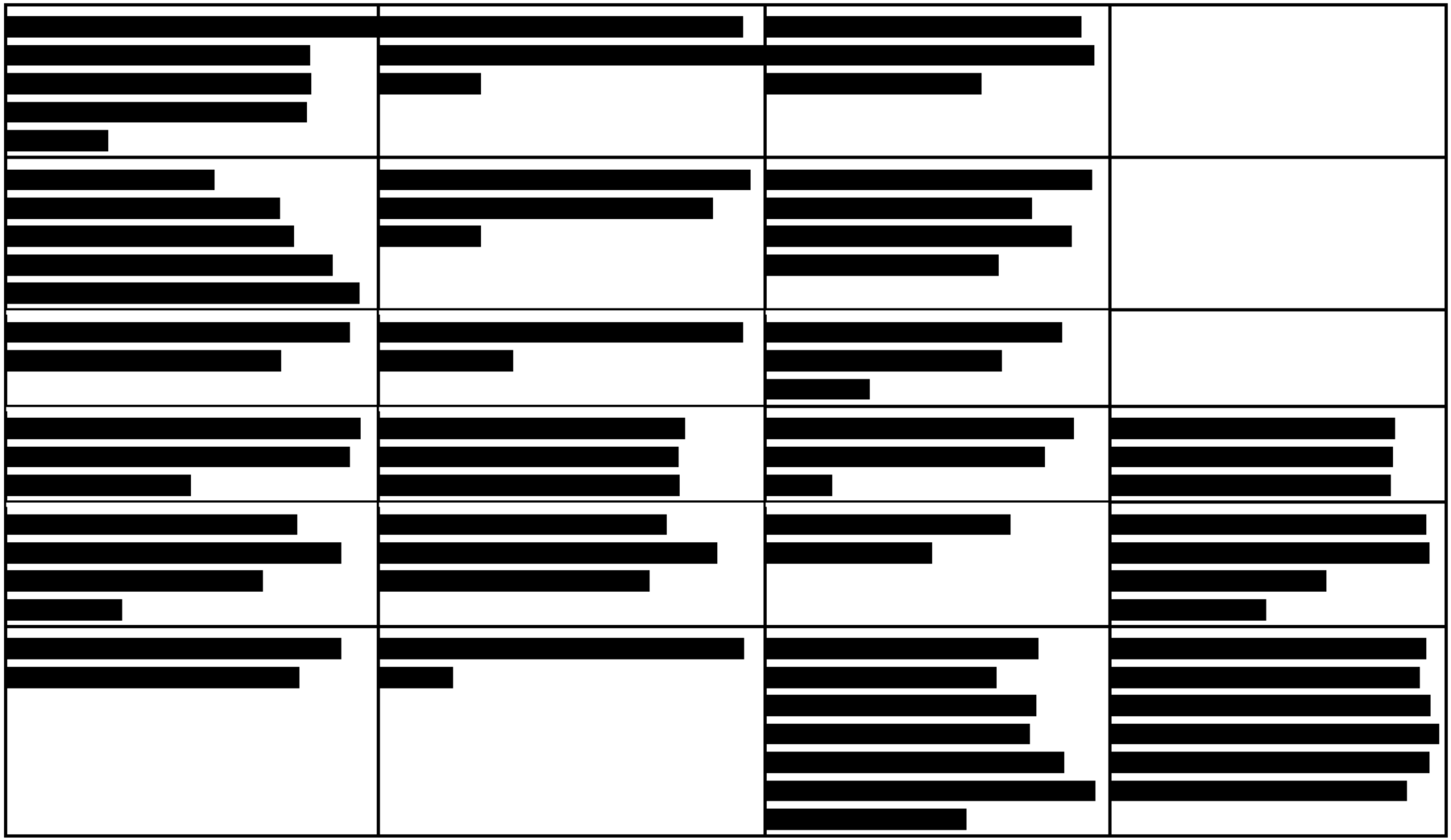


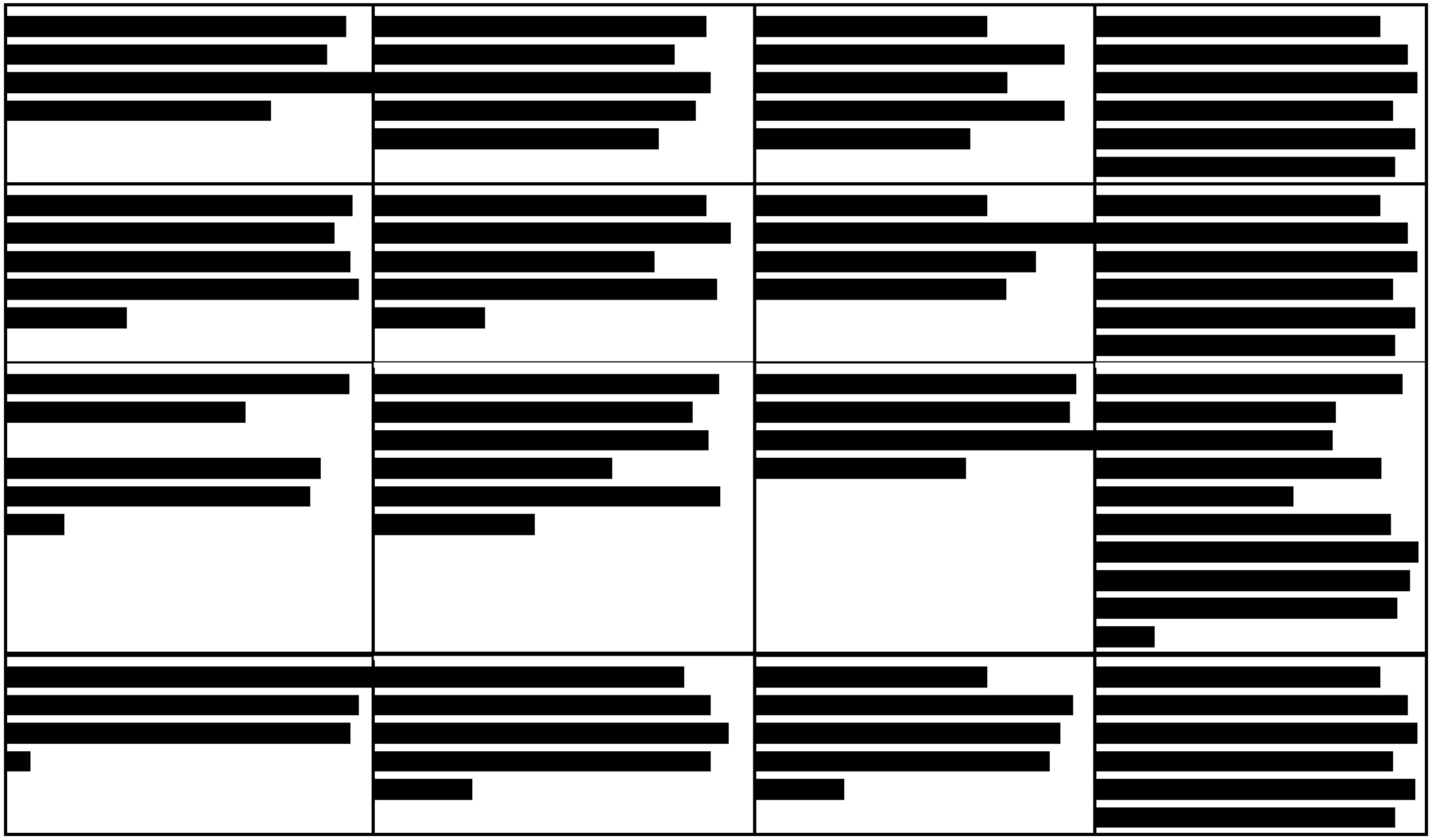
	[redacted]	[redacted]

6.6. ANÁLISIS DE BRECHA

Dirección General, DGRU			
Identificador único	DG3		
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		





6.7. PLAN DE TRABAJO

Dirección General, DGRU				
Identificador único	DG3			
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

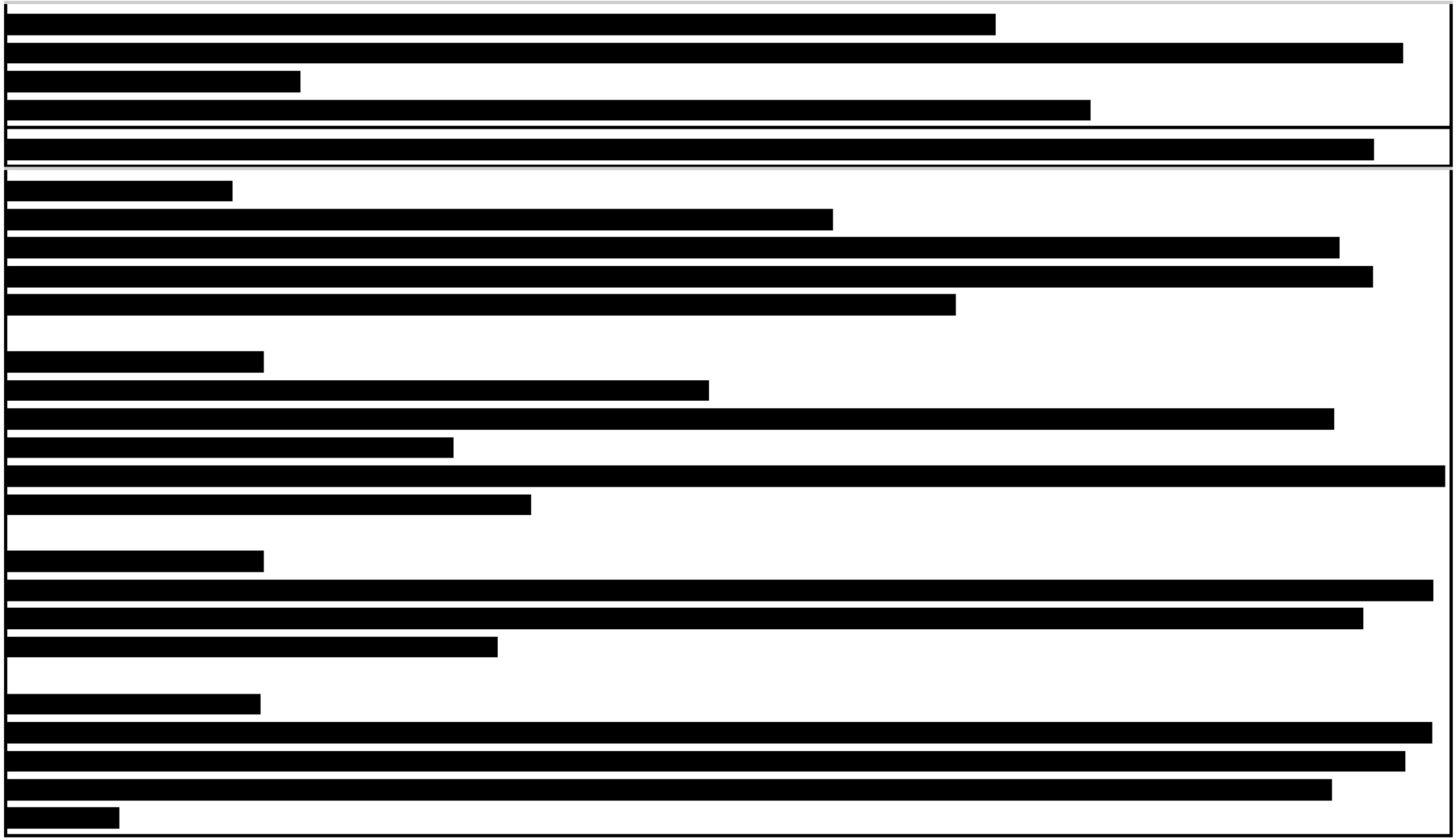
[redacted]	[redacted]		[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

6.8. MEDIDAS DE SEGURIDAD

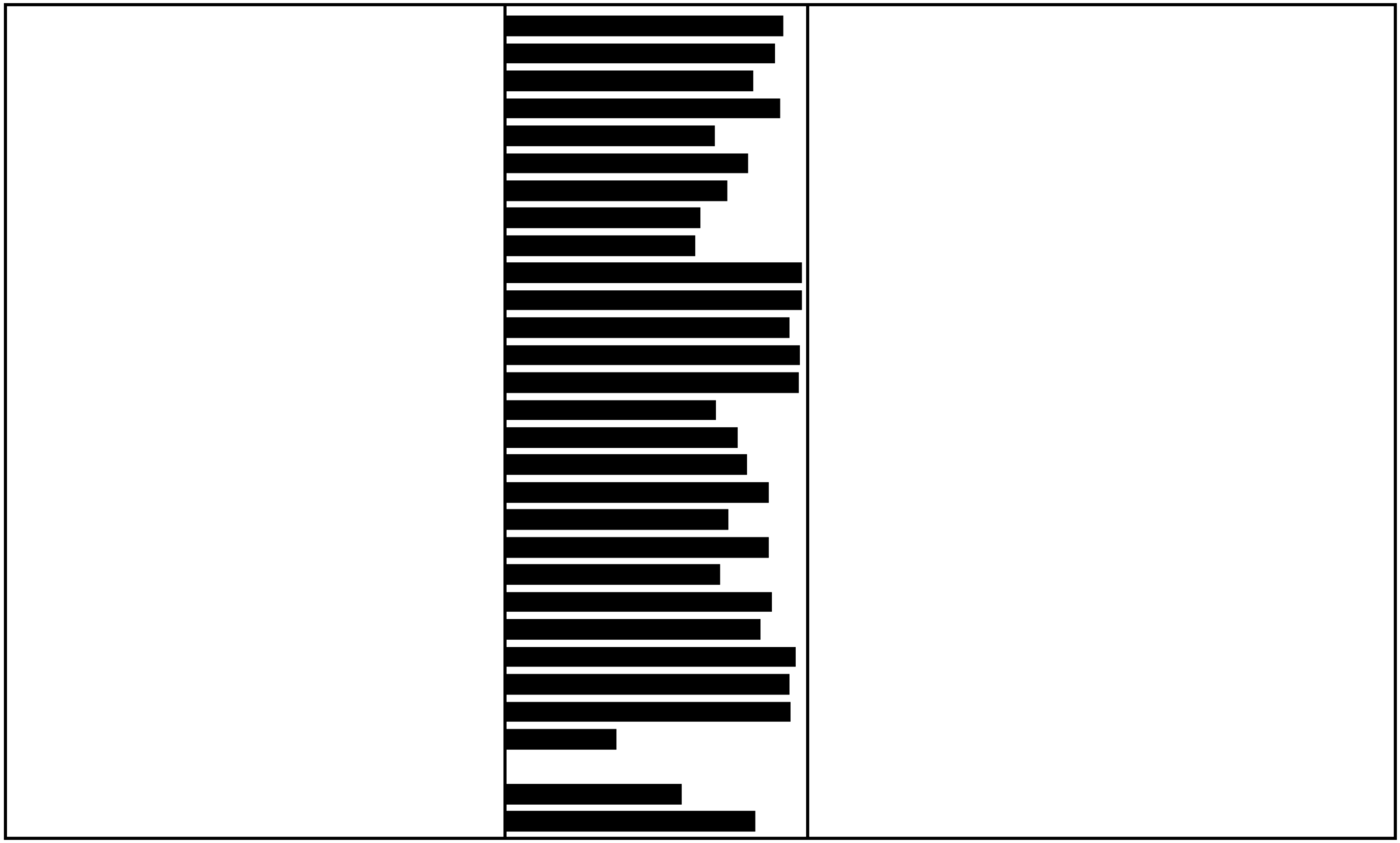
Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

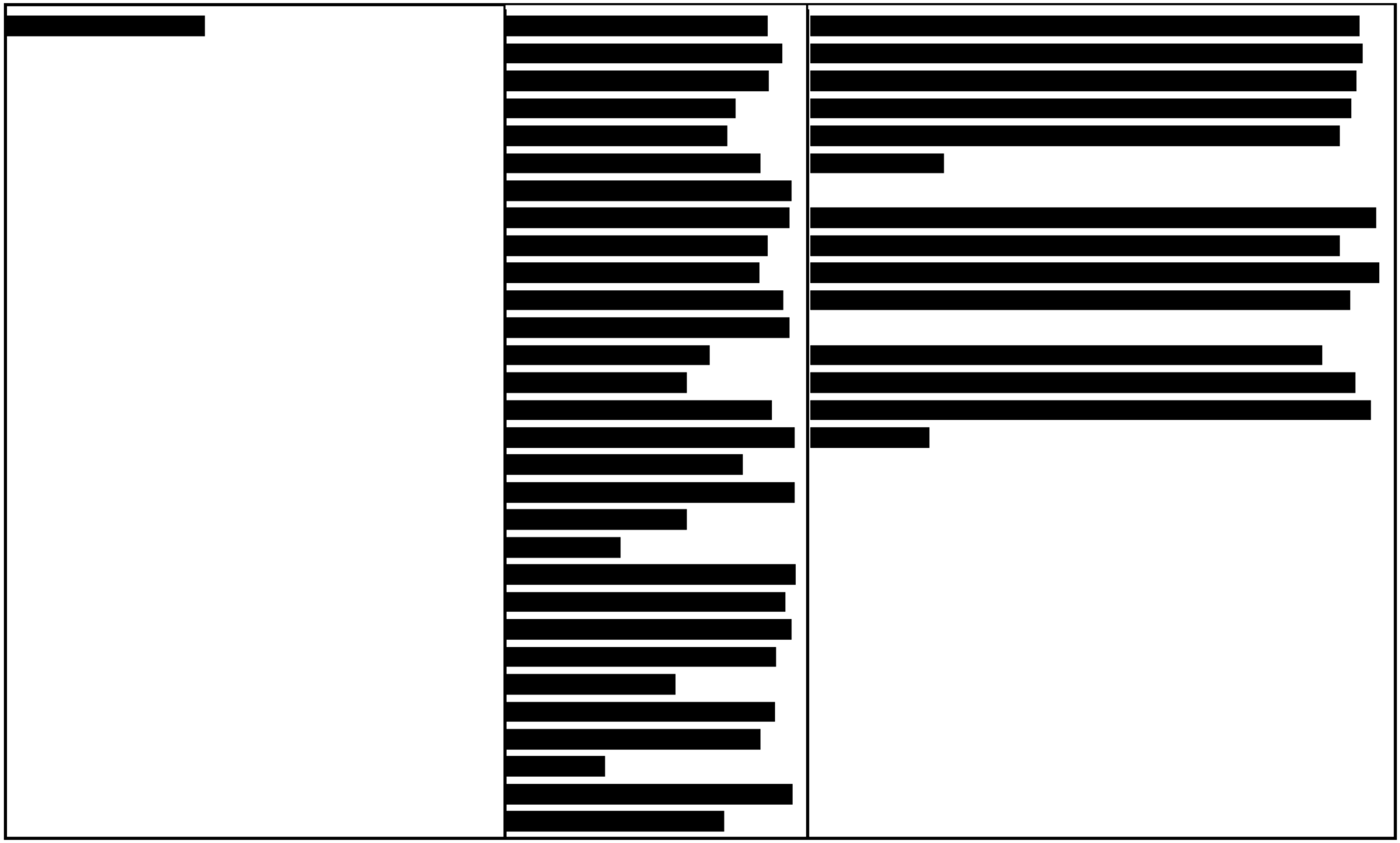
	[redacted]	

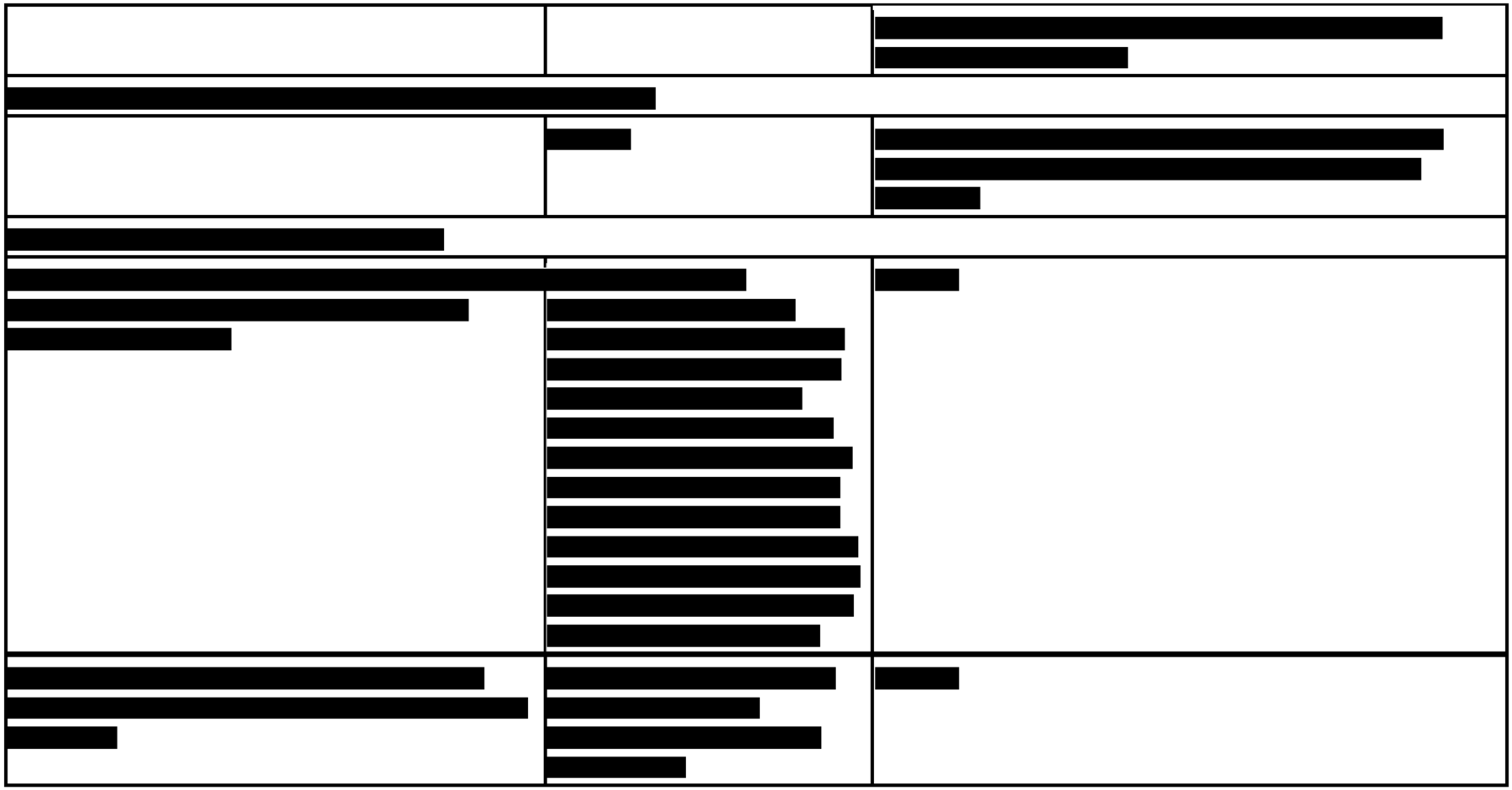
Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	



Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]







Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

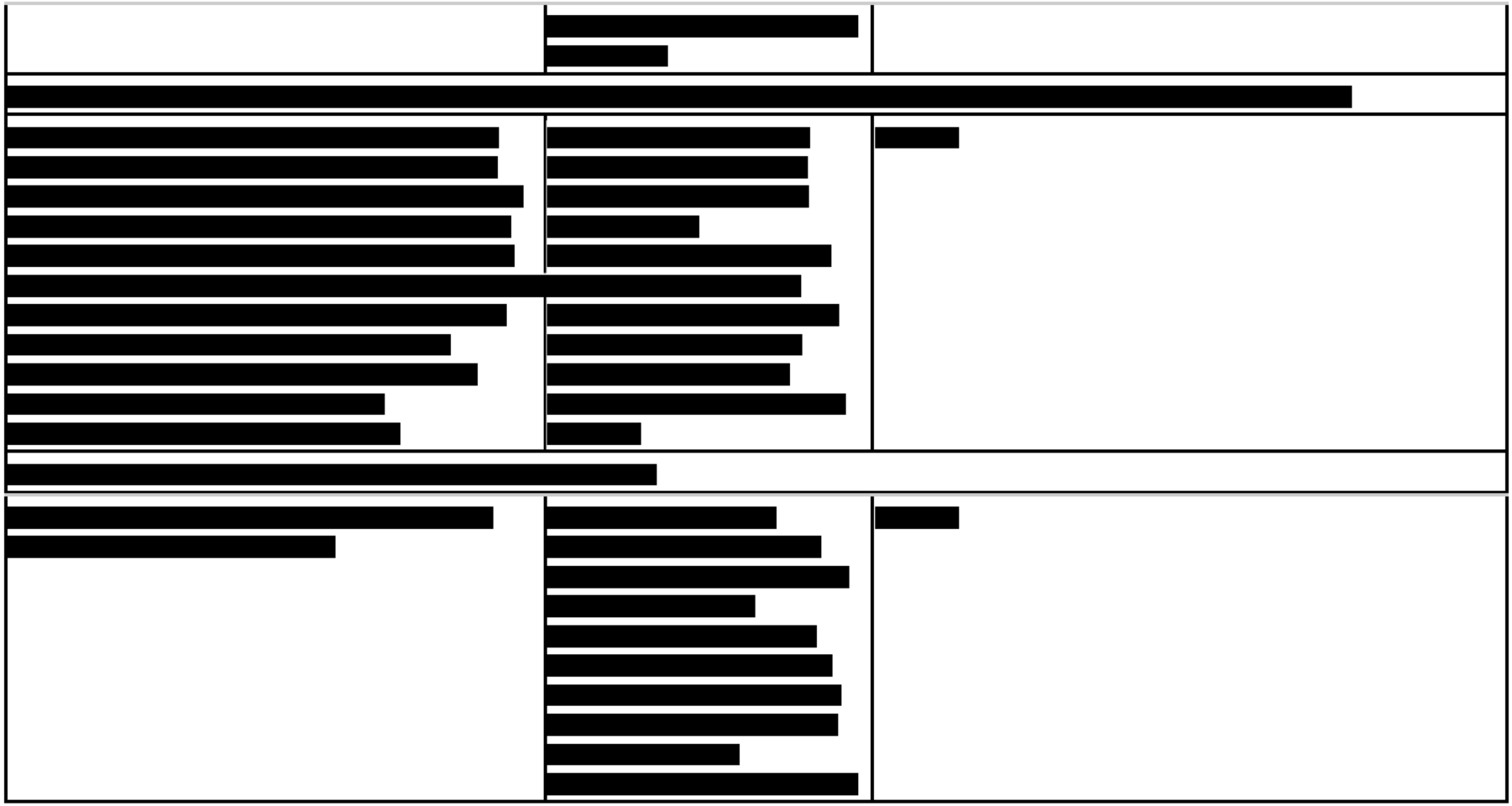
[redacted]		
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos
V. ACCESO A LAS INSTALACIONES	

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]

	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

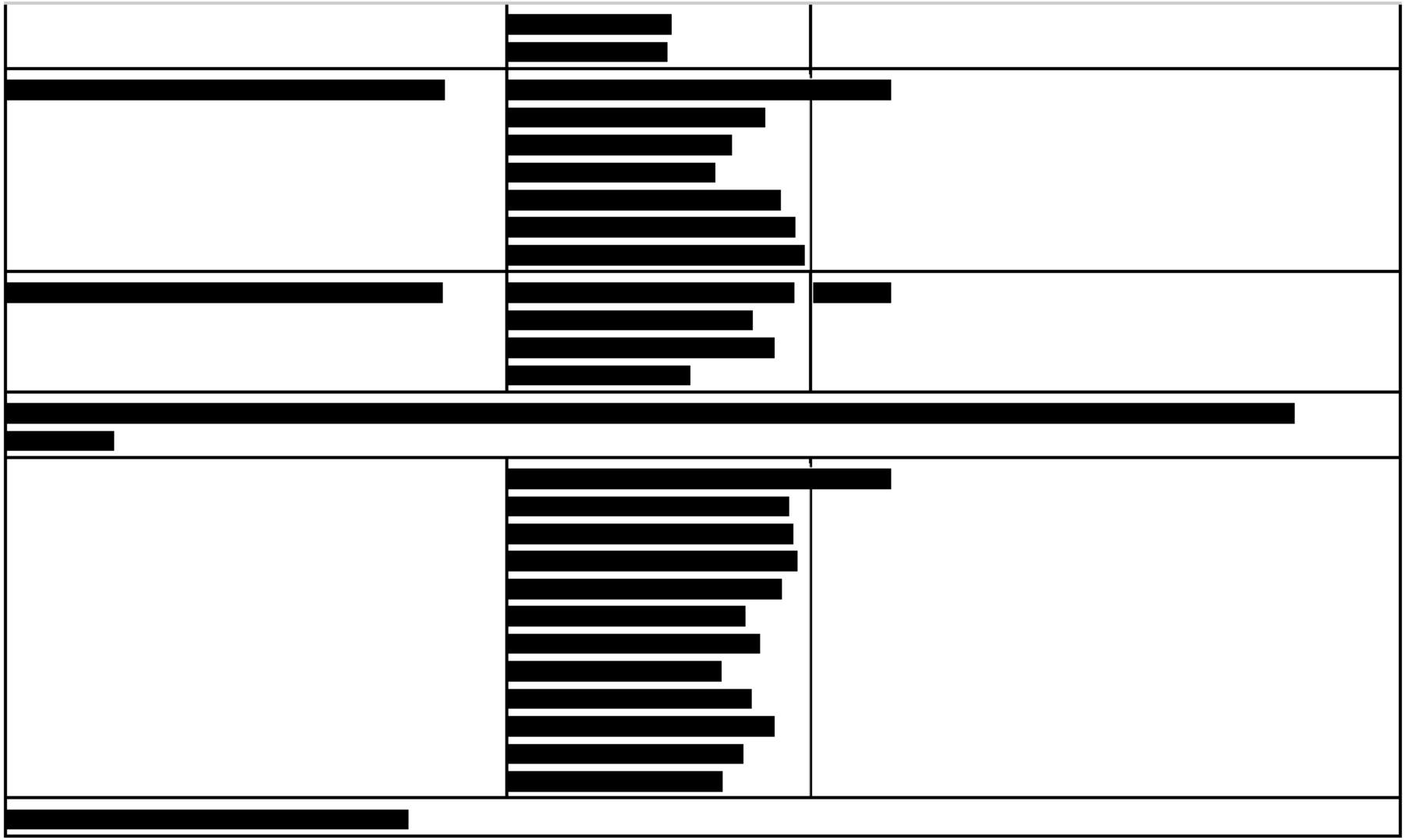
Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]

	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]

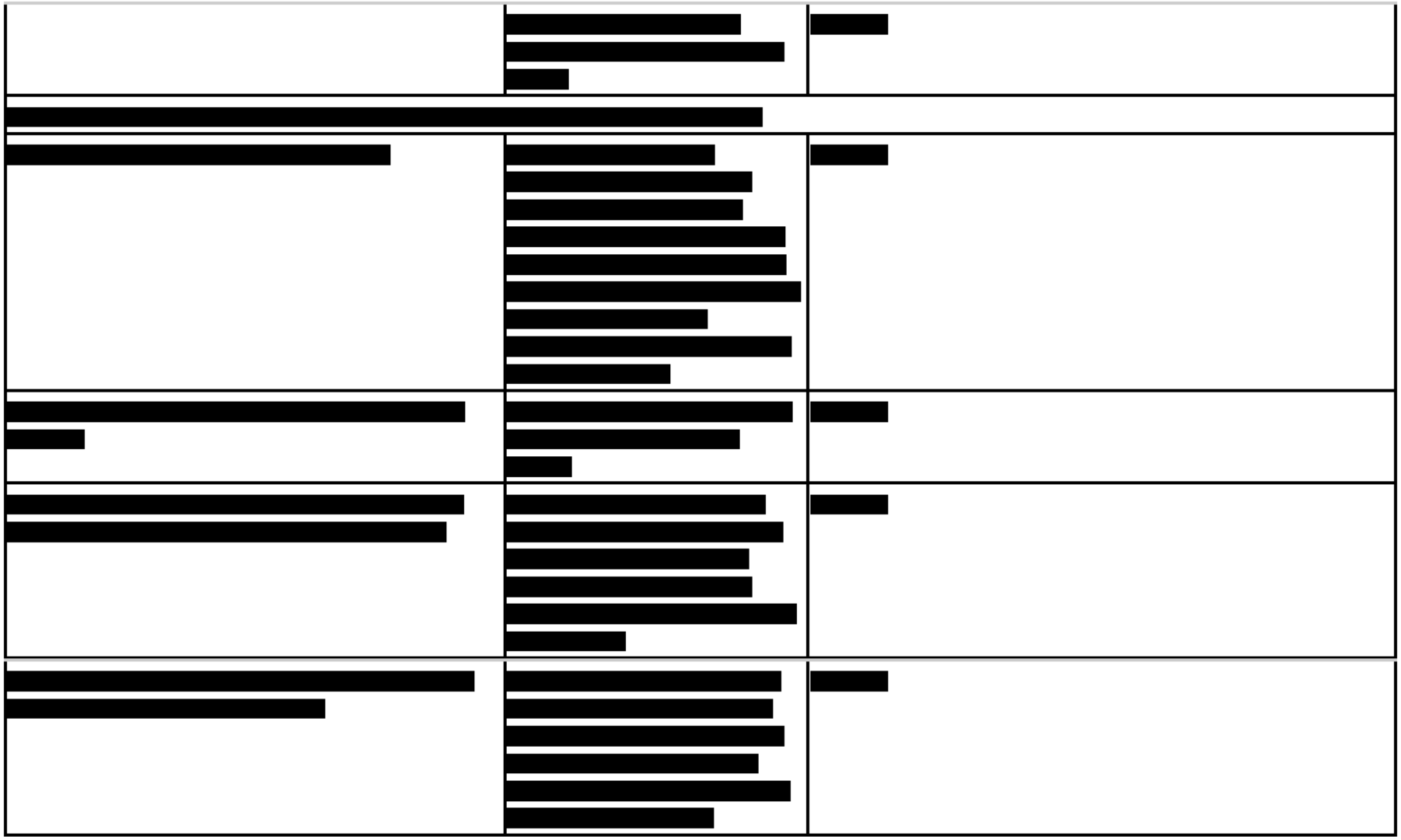
Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]



	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	[redacted]
[redacted]		



	[redacted]	

6.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General, DGRU		
Identificador único	DG3	
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Dirección General, DGRU	
Identificador único	DG3
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos

Medida de seguridad	Acciones	Responsable
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

6.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU				
Identificador único	DG3			
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media

Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Dirección General, DGRU				
Identificador único	DG3			
Nombre del sistema DG3	Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales - Procedimientos de borrado seguro de correos electrónicos y de archivos. - Dar a conocer el nombre de las personas autorizadas para acceder al	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones de Colecciones y Datos de Investigación, Sistema de Repositorios Universitarios, Desarrollo Tecnológico e Infraestructura, y de Planeación, Gestión y Normatividad involucrado con el tratamiento de datos personales. Frecuencia de la actualización una vez al año o antes si se	Alta

archivo y divulgarla al menos una vez al año. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.			considera necesario.	

Anexo 7. SRU1 Repositorio Institucional de la UNAM

7.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: Nombre. 1b. Datos laborales: Adscripción, cargos, domicilio de trabajo, correo electrónico institucional y teléfono institucional. 1c. Datos académicos: Trayectoria educativa, títulos y reconocimientos.	
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X)	
¿Para qué se usan?	El nombre completo, adscripción, puesto, correo electrónico institucional, trayectoria educativa, títulos y reconocimientos se publican como metadatos asociados a recursos digitales.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal (X) Gobierno Estatal (X) Gobierno Municipal (X) Personas físicas (X) Personas morales (X) Áreas Universitarias (X)	Los datos que se publican como metadatos asociados a recursos digitales, son cosechables mediante protocolos de interoperabilidad.
¿Dónde se alojan?	[redacted]	

¿Cuánto tiempo se da tratamiento?	Desde que los datos son cosechados hasta que el registro esté publicado en el repositorio. El registro completo y/o los metadatos con datos personales, pueden ser dados de baja mediante una indicación de la Unidad de Transparencia de la UNAM, a solicitud del proveedor de datos o del titular de los recursos digitales, en cuyo caso la información es eliminada de forma segura de todas las bases de datos de la DGRU en que se encuentre.
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Revisar que los datos personales contenidos en los metadatos que describen los recursos digitales se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos.
Obligaciones:	Recibir el conjunto de datos con los registros de los recursos digitales o la indicación de cosecharlos del repositorio del proveedor de datos. Supervisar la integración de los registros a la base de datos de trabajo y la ejecución de las solicitudes de baja, así como la integración del conjunto de datos depurado a las fuentes de datos del Repositorio Institucional UNAM. Supervisar que todo el proceso se realice en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Rubén Ignacio Sáenz González
Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Revisar que los datos personales contenidos en los metadatos que describen los recursos digitales se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos.

Obligaciones:	Emite la indicación de cosechar el repositorio de los recursos digitales; supervisa la depuración de los mismos y su integración final al Repositorio Institucional UNAM. Recibir y comunicar al Coordinador de Desarrollo Tecnológico e Infraestructura las solicitudes de baja. En algunos casos, realizar el proceso de cosecha bajo las medidas de seguridad técnicas necesarias. Realizar todos los procesos sin comprometer la integridad de los datos personales.
Co-Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad
Funciones:	Verificar que se haya eliminado el acceso a los datos personales, en atención a las solicitud de baja por parte de la Unidad de Transparencia de la UNAM.
Obligaciones:	Recibir las solicitudes de baja de parte de la Unidad de Transparencia de la UNAM, transmitirlas al Coordinador del Sistema de Repositorios Universitarios. Una vez atendida la solicitud, responder a la Unidad de Transparencia de la UNAM. Realizar el proceso sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Oscar Hernández Hernández
Cargo:	Jefe de Departamento de Instalación y Soporte de Repositorios Universitarios
Funciones:	Organizar y almacenar los datos personales contenidos en los metadatos que describen los recursos digitales y los datos del directorio, sin comprometer la integridad de los mismos.
Obligaciones:	Revisar que los datos personales contenidos en los metadatos que describen los recursos digitales y los del directorio se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos.

	Una vez procesados los datos de cosecha realiza labores de catalogación, normalización y limpieza de datos. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	Efraín Hipólito Chamú
Cargo:	No aplica
Funciones:	Obtener, registrar, organizar y almacenar los datos personales contenidos en los metadatos que describen los recursos digitales sin comprometer la integridad de los mismos.
Obligaciones:	Realiza la cosecha de datos y organiza la información para el proceso de integración al esquema del Repositorio Institucional UNAM. Una vez que los datos son depurados, ejecuta el proceso de propagación hacia las fuentes de datos que alimentan a la plataforma del Repositorio Institucional UNAM. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Encargado	
Nombre:	Dulce Estefanía Rivera Díaz
Cargo:	No aplica
Funciones:	Registrar, organizar y almacenar los datos personales contenidos en los metadatos que describen los recursos digitales sin comprometer la integridad de los mismos.
Obligaciones:	Recibe el conjunto de datos cosechados y los procesa para su integración al esquema del Repositorio Institucional UNAM. Prepara las tablas que posteriormente serán depuradas. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la

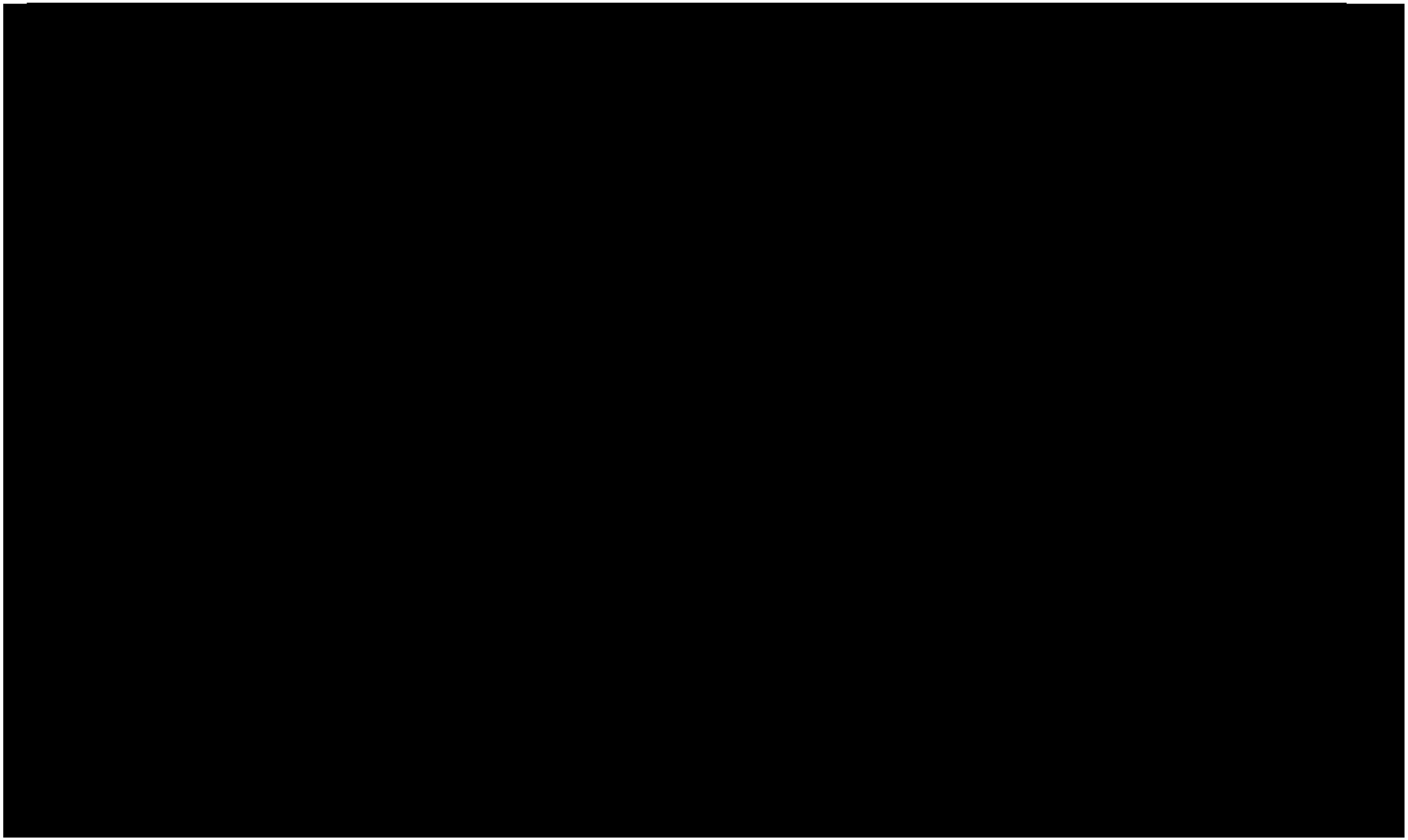
	integridad de los datos personales.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Encargado	
Nombre:	Karina Anahi López Coca
Cargo:	No aplica
Funciones:	Organizar y almacenar los datos personales contenidos en los metadatos que describen los recursos digitales y los datos del directorio, sin comprometer la integridad de los mismos.
Obligaciones:	Revisar que los datos personales contenidos en los metadatos que describen los recursos digitales y los del directorio se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos. Una vez procesados los datos de cosecha realiza labores de catalogación, normalización y limpieza de datos. Cuando su proceso concluye, da aviso al Coordinador del Sistema de Repositorios Universitarios para que los datos sean integrados al esquema del Repositorio Institucional UNAM. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	Mady Lizeth García Espino
Cargo:	No aplica
Funciones:	Organizar y almacenar los datos personales contenidos en los metadatos que describen los recursos digitales y los datos del directorio, sin comprometer la integridad de los mismos.
Obligaciones:	Revisar que los datos personales contenidos en los metadatos que describen los recursos digitales y los del directorio se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos.

	Una vez procesados los datos de cosecha realiza labores de catalogación, normalización y limpieza de datos. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	José Daniel Rivera Terrazas
Cargo:	No aplica
Funciones:	Organizar y almacenar los datos personales contenidos en los metadatos que describen los recursos digitales y los datos del directorio, sin comprometer la integridad de los mismos.
Obligaciones:	Revisar que los datos personales contenidos en los metadatos que describen los recursos digitales y los del directorio se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos. Una vez procesados los datos de cosecha realiza labores de catalogación, normalización y limpieza de datos. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	Karen Zavala Correa
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General

Encargado	
Nombre:	Laura Patricia Olguín Pérez
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	Mary Carmen Alva Pazarán
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Usuarios	
Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

7.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Sistema de Repositorios Universitarios, DGRU	
Identificador único	SRU1
Nombre del sistema SRU1	Repositorio Institucional de la UNAM
Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]



7.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Bases de datos de recursos digitales que pueden contener información personal	Los metadatos de los recursos digitales son primordiales pues se publican en el Repositorio Institucional de la UNAM, siendo éste una de las plataformas principales desarrolladas y administradas por la DGRU. Los datos personales asociados a los recursos digitales del repositorio, resultan esenciales para propósitos de identificación.	Bases de datos de recursos digitales que posiblemente contengan datos personales de identificación, laborales y académicos.
Dueño		
¿A quién pertenece el activo de información?		
Coordinador del Sistema de Repositorios Universitarios		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
( ) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente manera:	La información únicamente podrá ser modificada por personal autorizado de la DGRU.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera:	La información de las bases de datos de recursos digitales debe estar disponible

		para que el personal asignado realice las actividades designadas.
	Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	Los metadatos asociados a los recursos digitales publicados en el RI-UNAM deberán estar disponibles para su consulta.
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
( ) Confidencialidad	**(X) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]

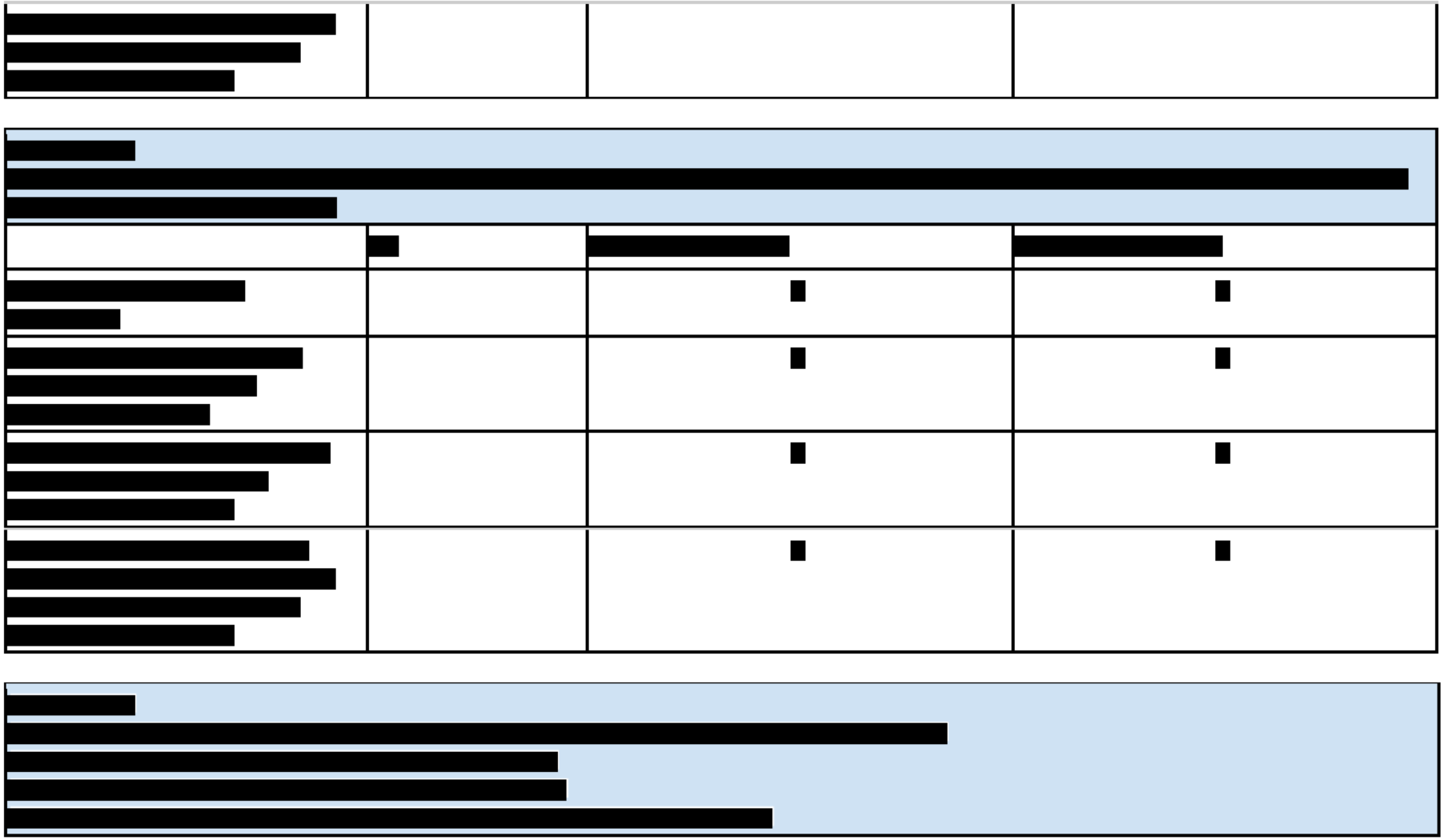
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	
[redacted]	
[redacted]	
[redacted]	
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	

7.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Repositorio Institucional de la UNAM
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			



[redacted]

CONTENEDORES FÍSICOS

[redacted]

RECURSOS HUMANOS

[redacted]

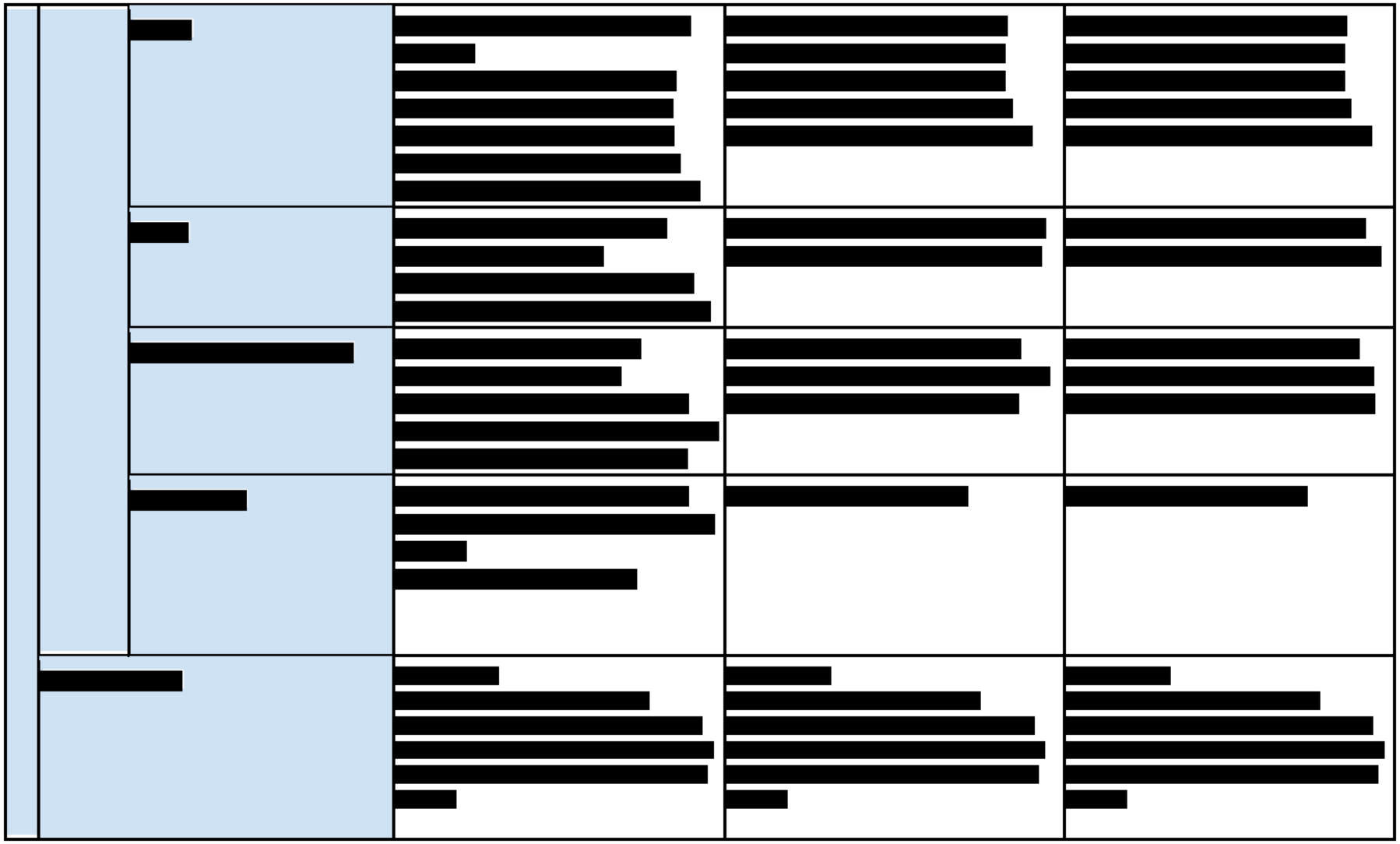
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

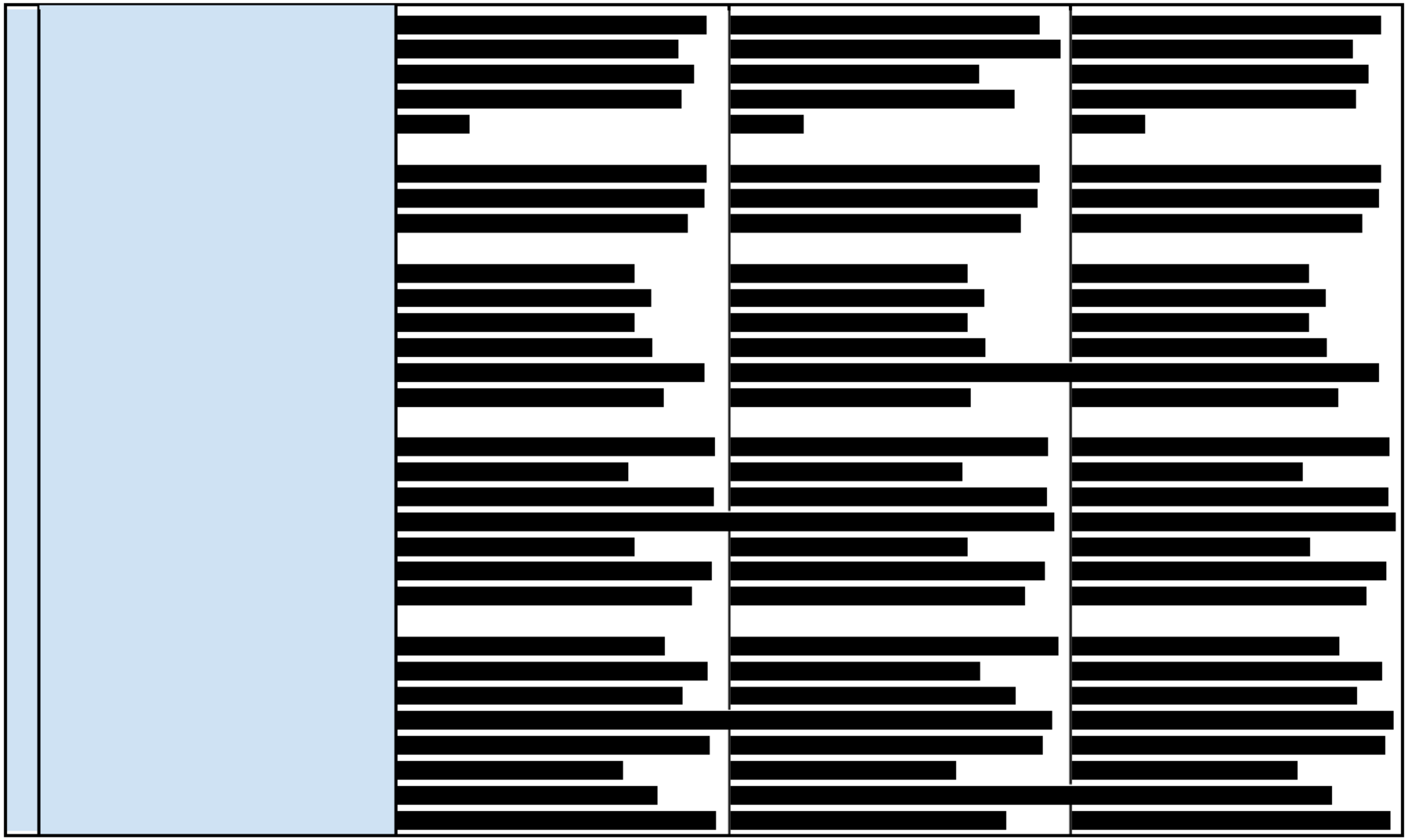
[redacted]			
	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

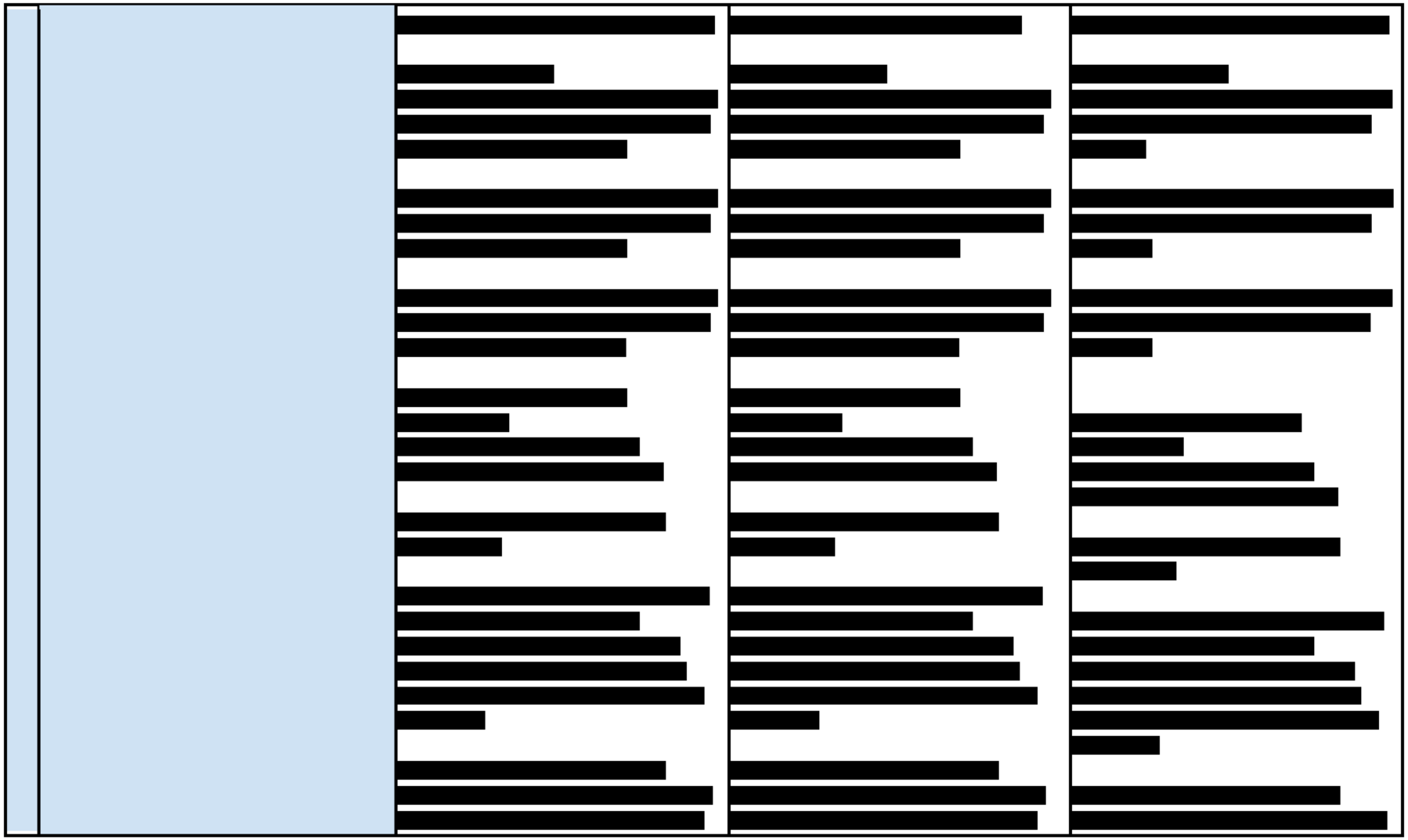
[redacted]			

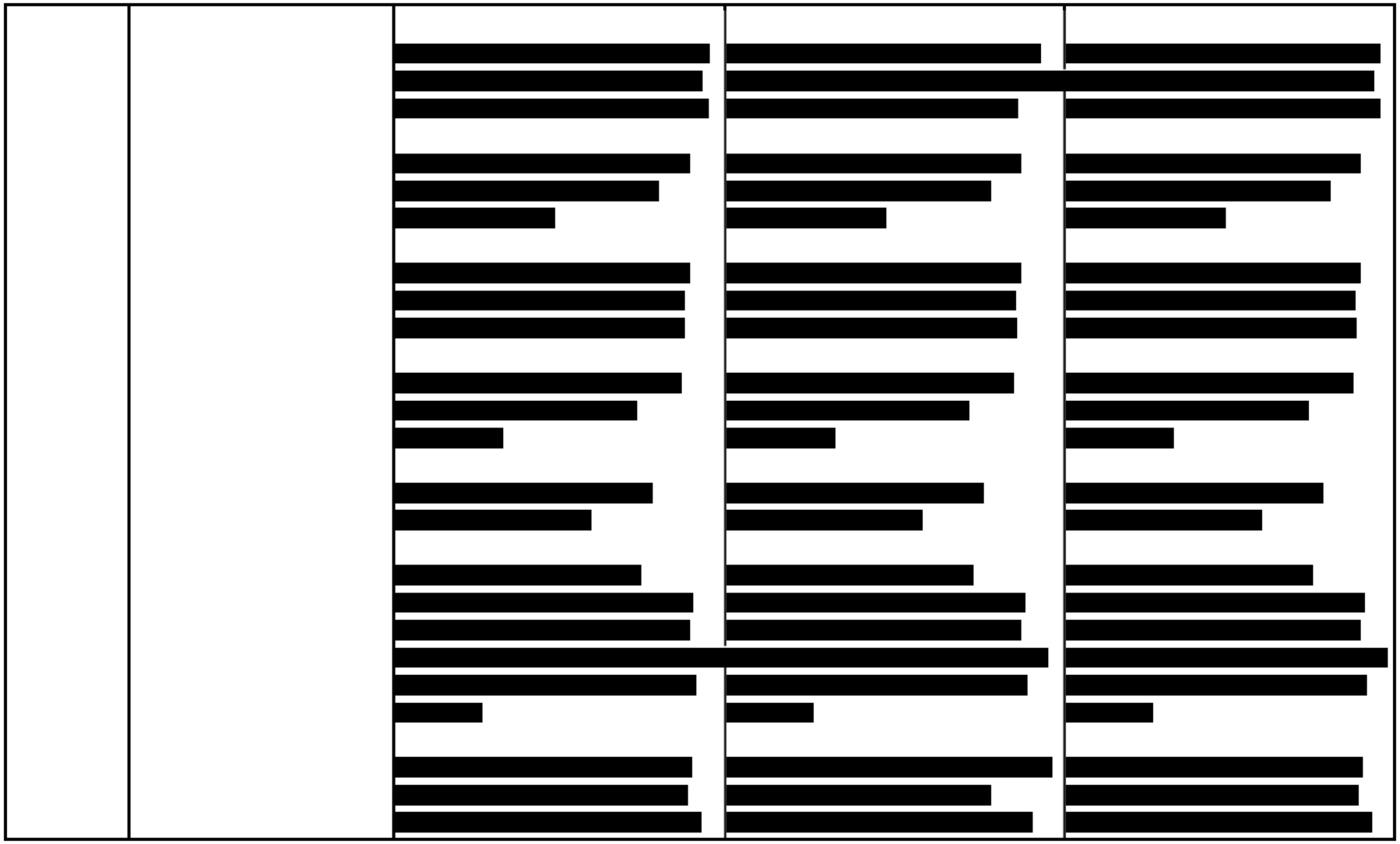
7.5. ANÁLISIS DE RIESGOS

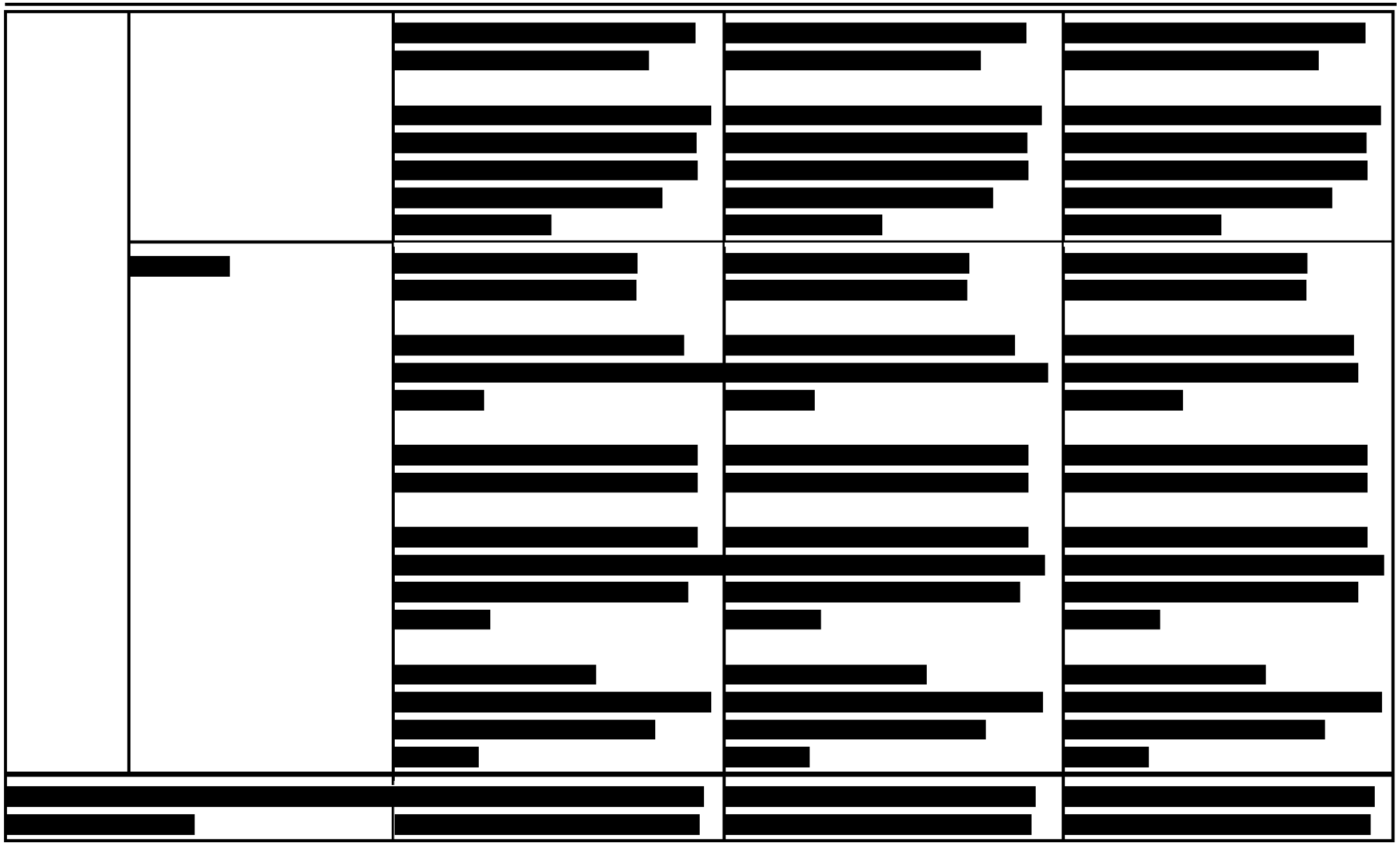
[redacted]

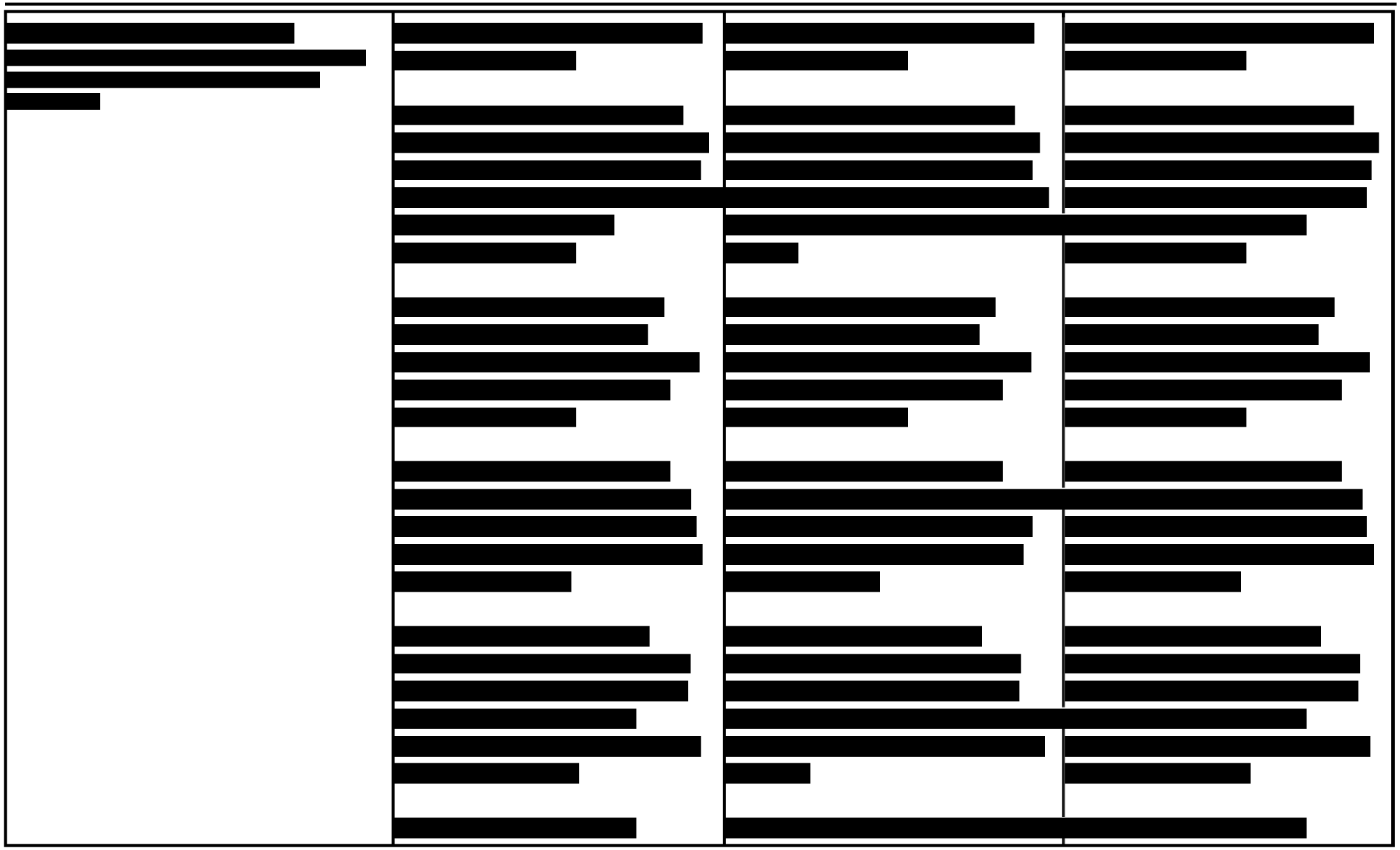










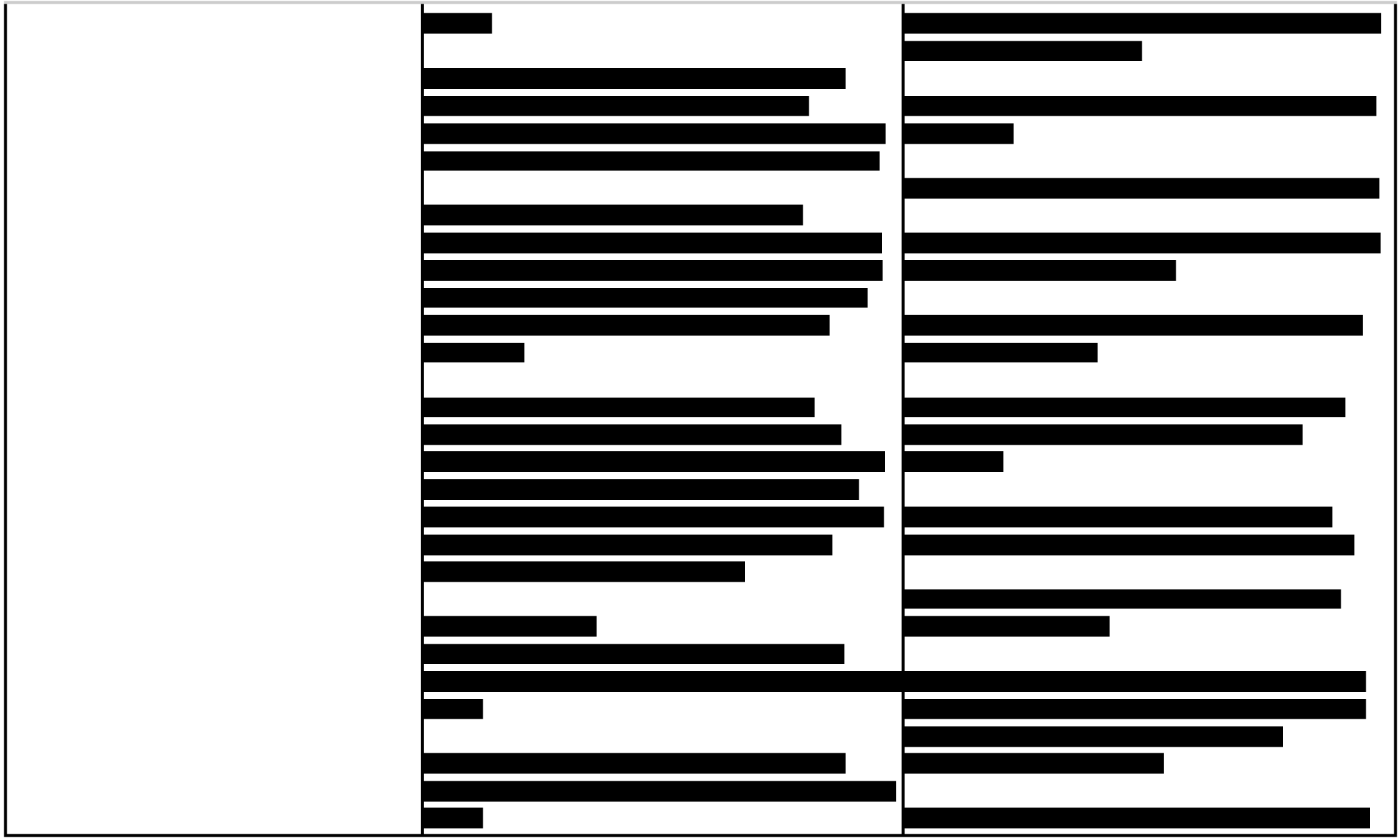


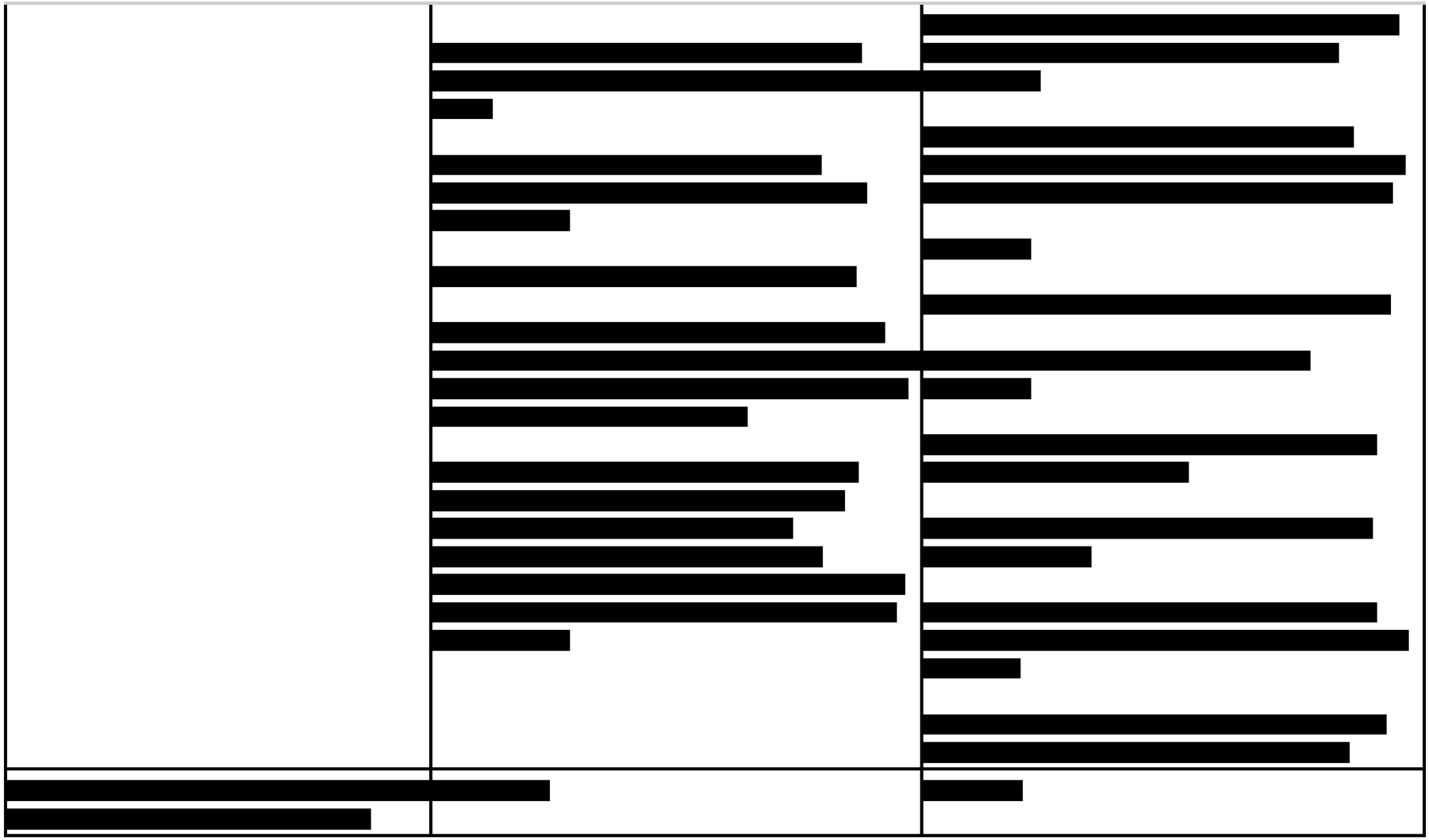
	[redacted]	[redacted]	[redacted]

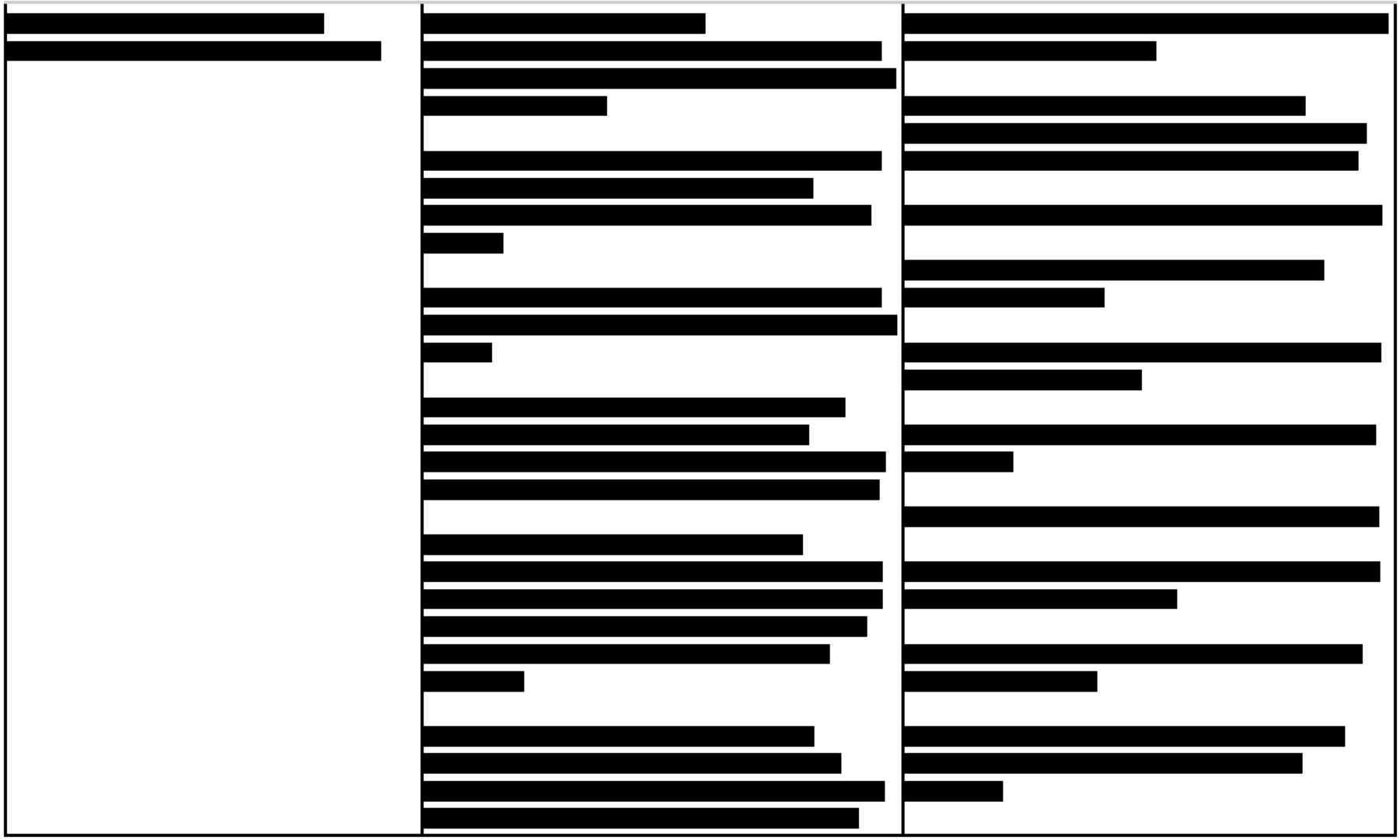
Sistema de Repositorios Universitarios, DGRU	
Identificador único	SRU1
Nombre del sistema SRU1	Repositorio Institucional de la UNAM

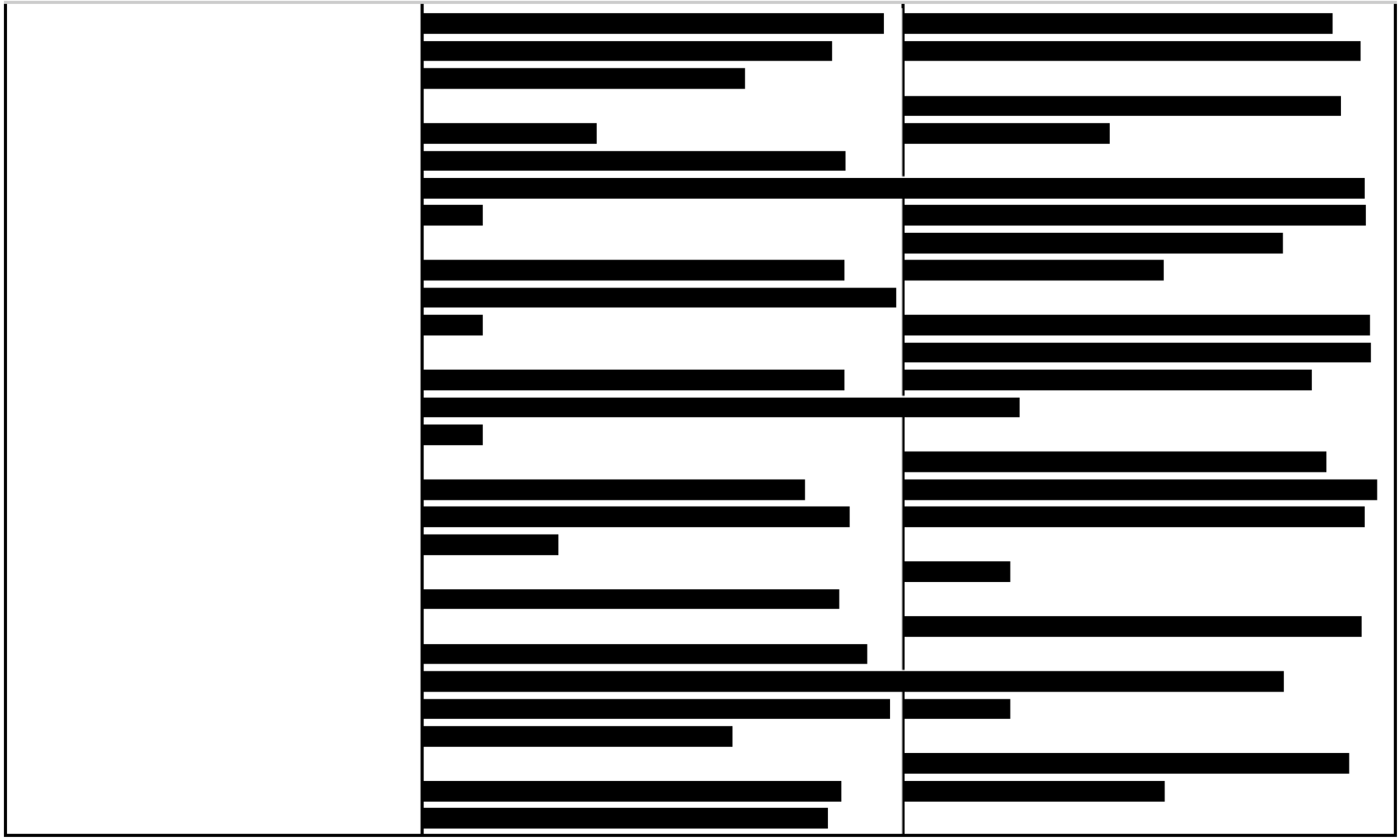
ANÁLISIS DE RIESGOS

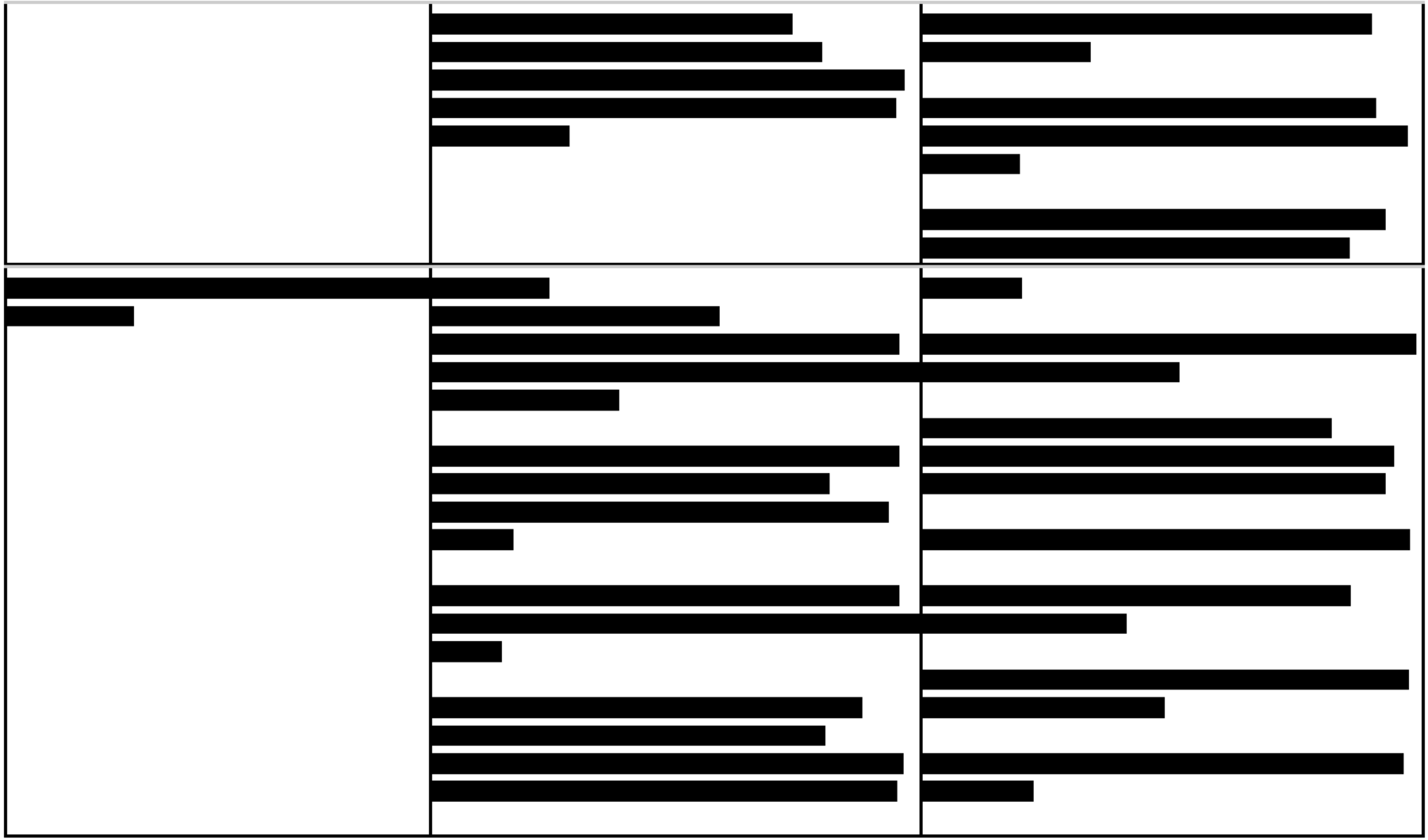
Riesgo	Impacto	Mitigación
[redacted]	[redacted]	[redacted]

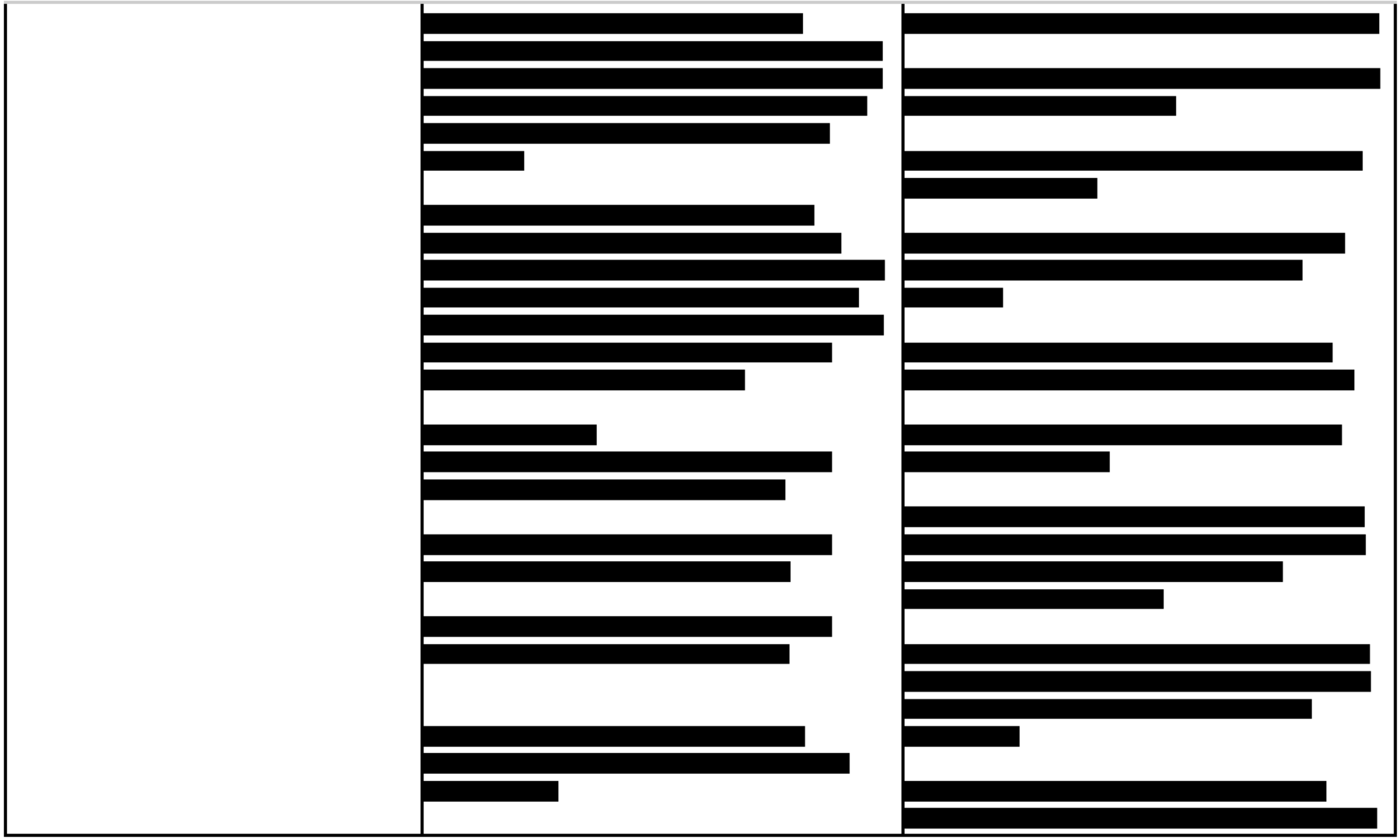


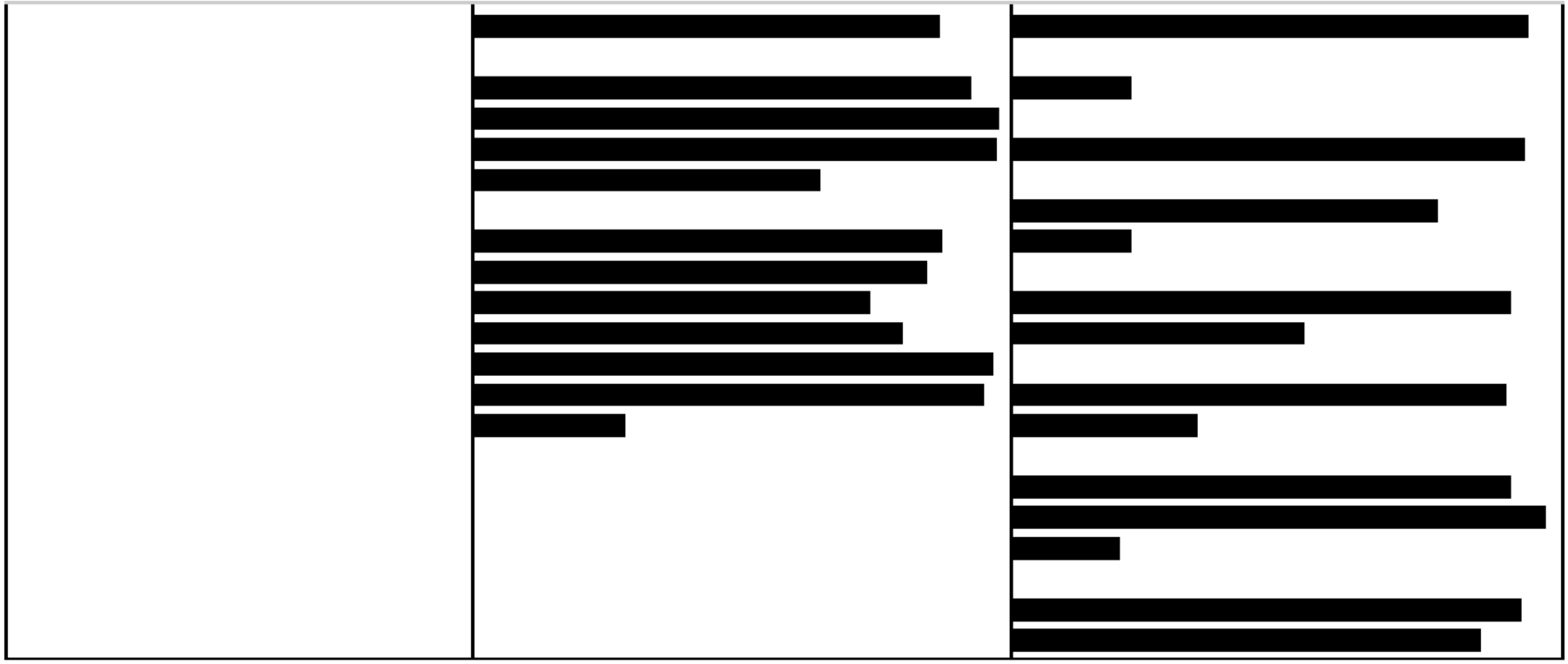










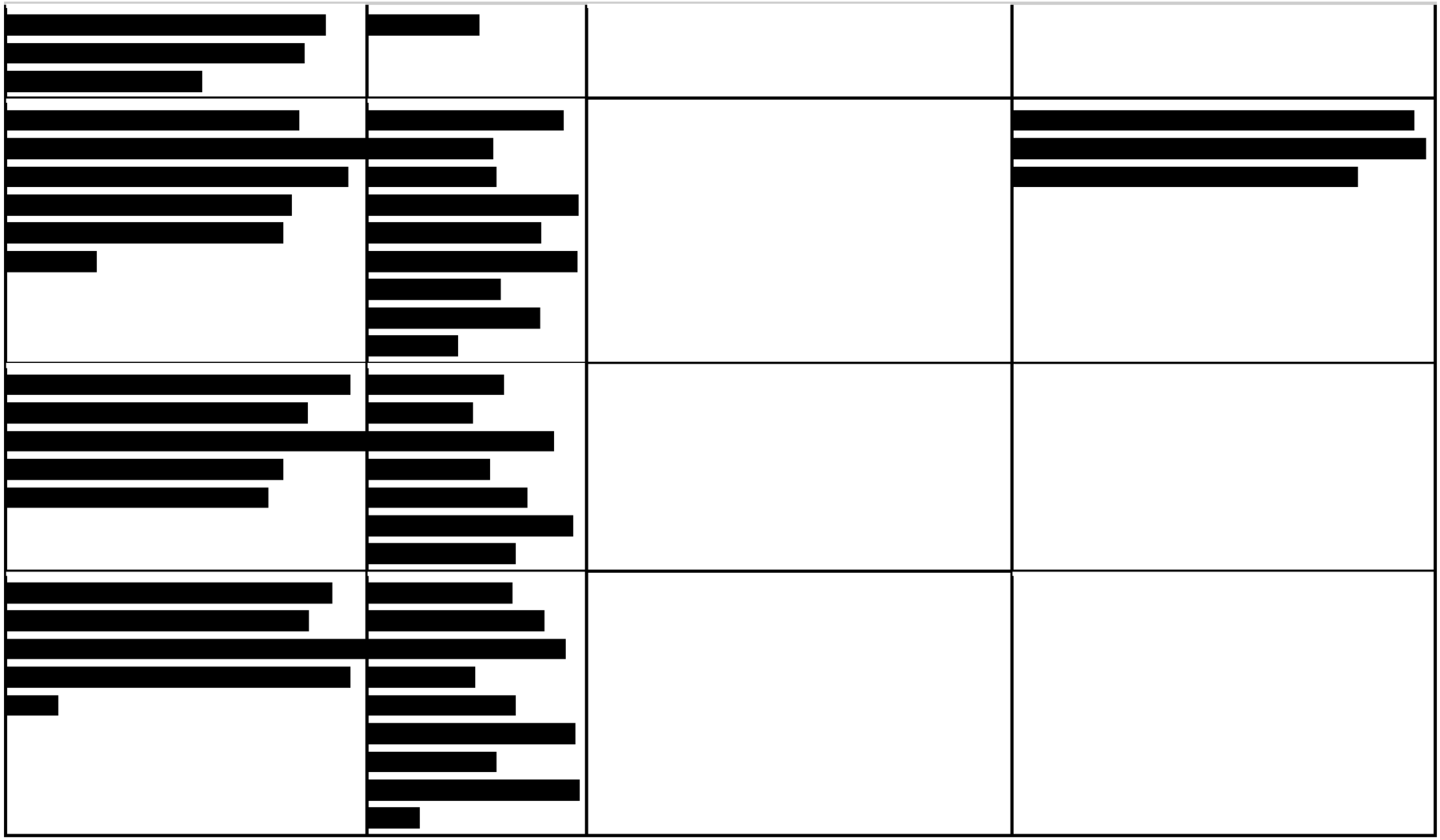


7.6. ANÁLISIS DE BRECHA

Sistema de Repositorios Universitarios, DGRU	
Identificador único	SRU1
Nombre del sistema SRU1	Repositorio Institucional de la UNAM

Medida de seguridad actual	Medida de seguridad necesaria	Acciones para remediación	¿Qué se necesita?
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			



7.7. PLAN DE TRABAJO

Sistema de Repositorios Universitarios, DGRU				
Identificador único	SRU1			
Nombre del sistema SRU1	Repositorio Institucional de la UNAM			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]			[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

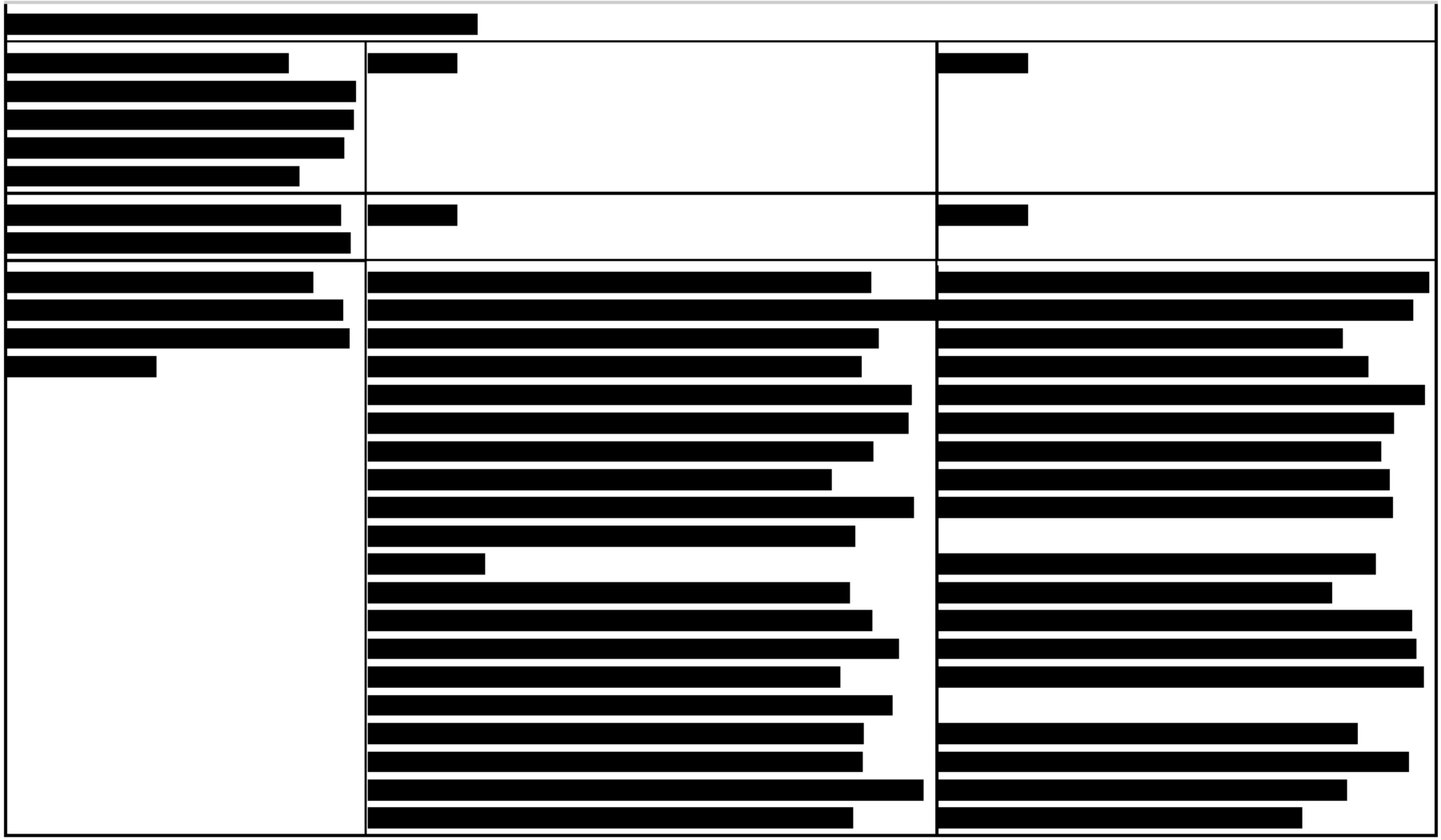
7.8. MEDIDAS DE SEGURIDAD

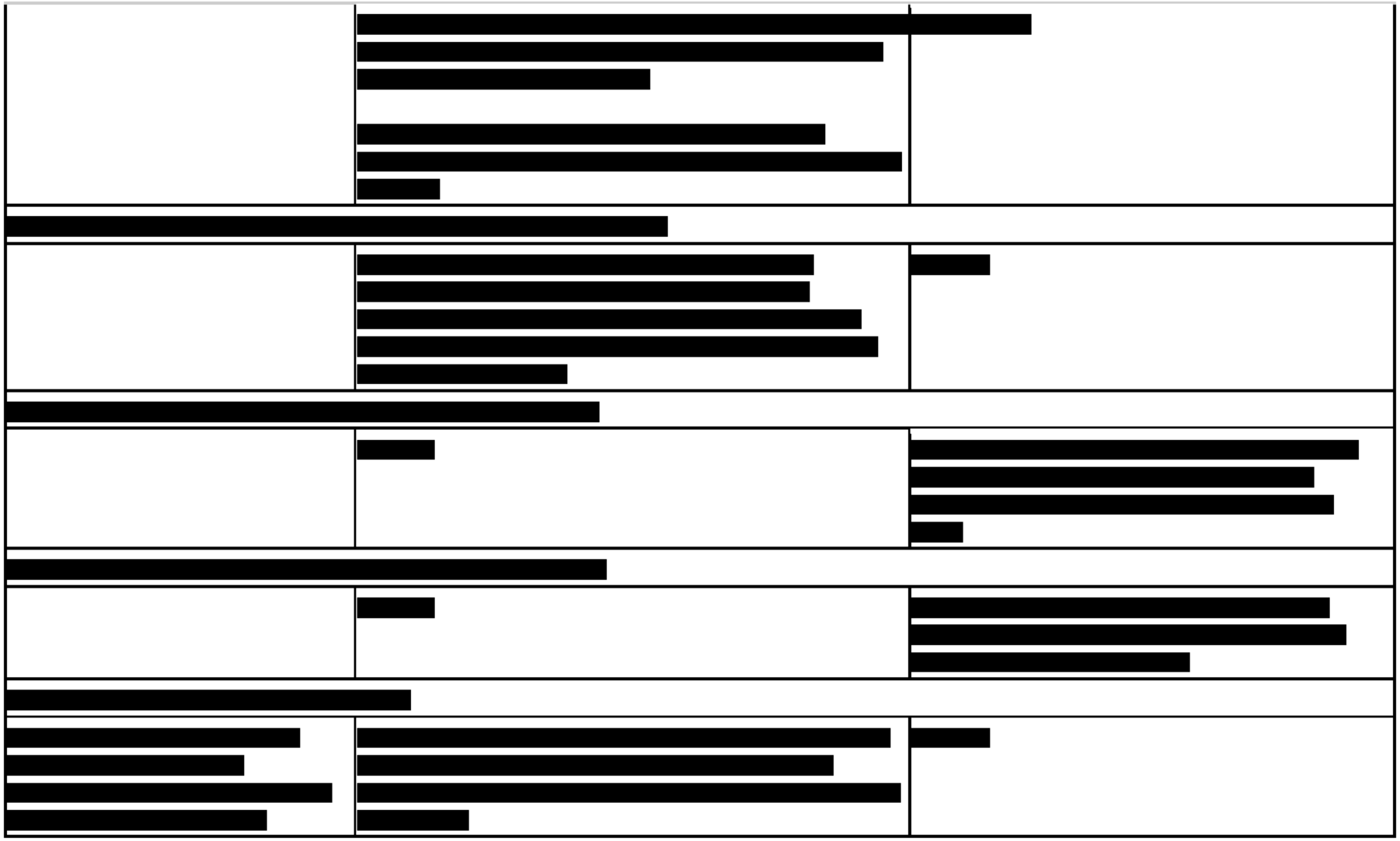
Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	

Sistema de Repositorios Universitarios, DGRU	
Identificador único	SRU1
Nombre del sistema SRU1	Repositorio Institucional de la UNAM
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**





[redacted]	[redacted]	[redacted]

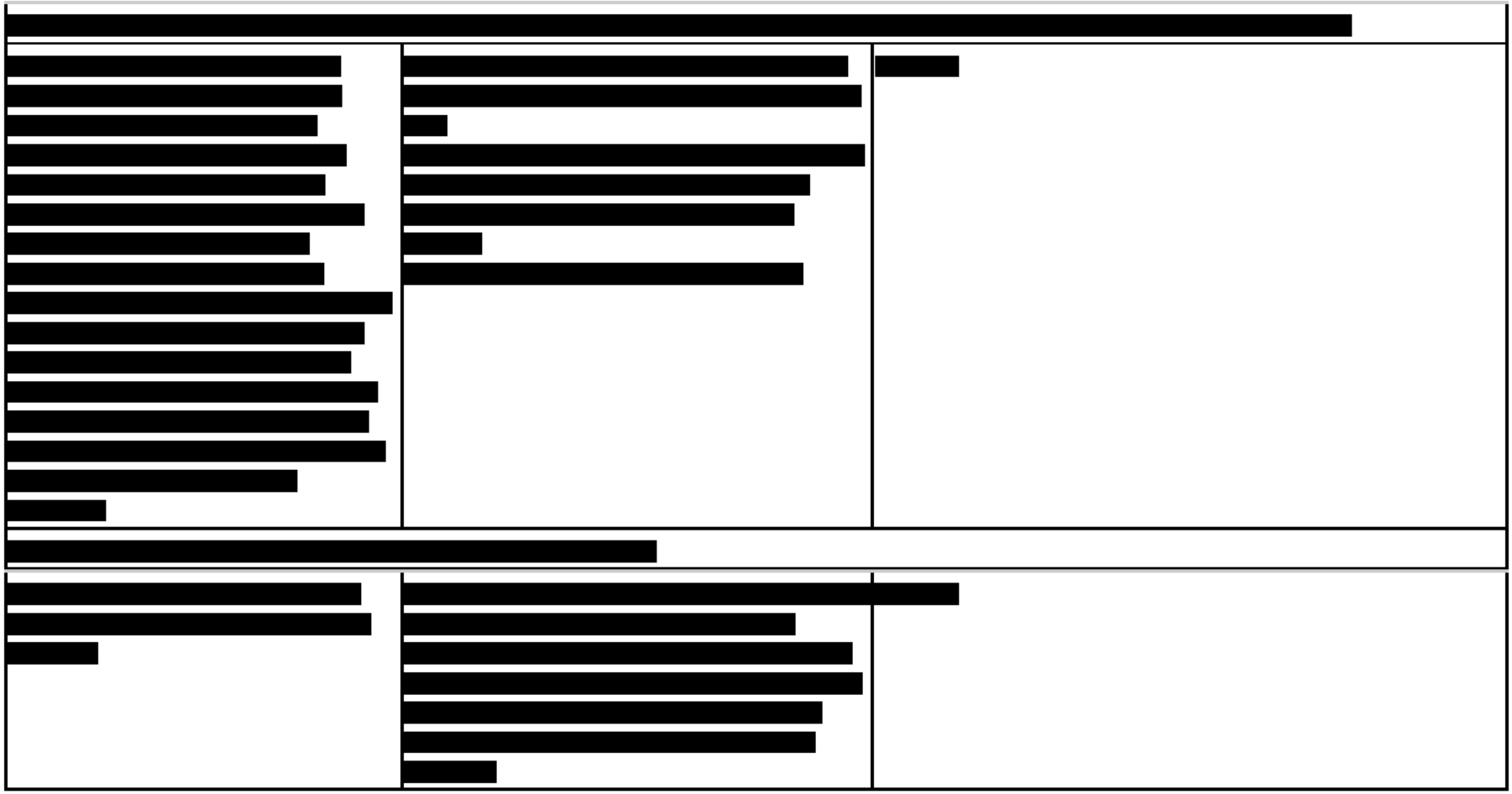
Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		de [redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

[redacted]		
	[redacted]	[redacted]

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]

	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



Sistema de Repositorios Universitarios, DGRU	
Identificador único	SRU1

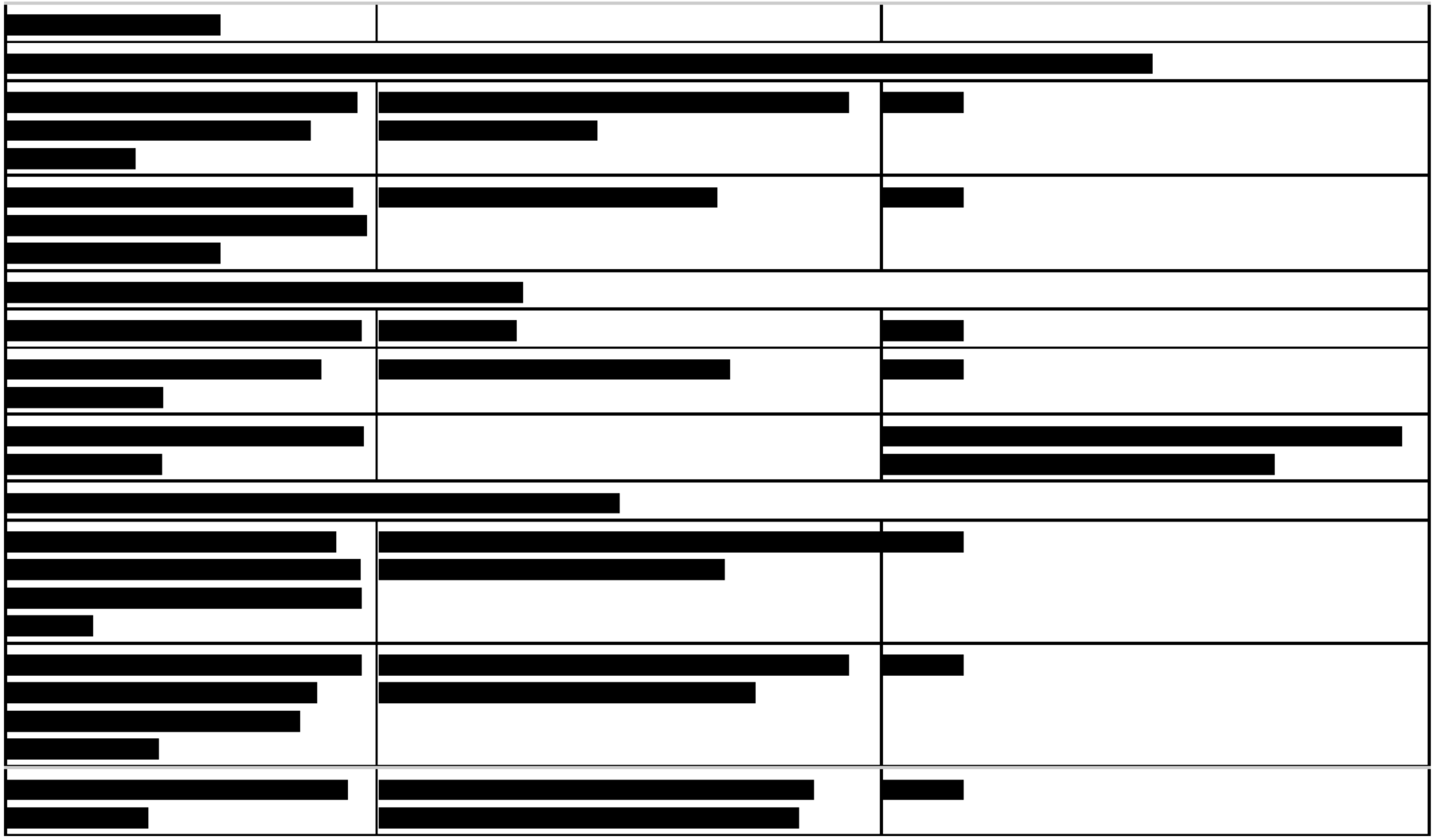
Nombre del sistema SRU1	Repositorio Institucional de la UNAM

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

Sistema de Repositorios Universitarios, DGRU	
Identificador único	SRU1
Nombre del sistema SRU1	Repositorio Institucional de la UNAM

VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]

	[redacted]	
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



	[redacted]	

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		

	[redacted]	
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

7.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Sistema de Repositorios Universitarios, DGRU

Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Sistema de Repositorios Universitarios, DGRU		
Identificador único	SRU1	
Nombre del sistema SRU1	Repositorio Institucional de la UNAM	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

7.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Sistema de Repositorios Universitarios, DGRU				
Identificador único	SRU1			
Nombre del sistema SRU1	Repositorio Institucional de la UNAM			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Sistema de Repositorios Universitarios, DGRU

Identificador único	SRU1			
Nombre del sistema SRU1	Repositorio Institucional de la UNAM			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales. - Procedimientos de borrado seguro de correos electrónicos y de archivos. - Uso adecuado de datos personales durante el desarrollo involucrado en las bases de datos que los contienen. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones del Sistema de Repositorios Universitarios y Desarrollo Tecnológico e Infraestructura involucrado en la operación del Repositorio Institucional de la UNAM. Frecuencia de la actualización una vez al año o antes si se considera necesario.	Alta

Anexo 8. CDI1 Portal de Datos Abiertos UNAM, Colecciones Universitarias

8.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: nombre completo. 1b. Datos laborales: institución, puesto, correo electrónico institucional, teléfono institucional, usuario, perfil y contraseña.	
¿Cómo se obtienen los datos personales?	Físico (X) Digital (X)	
¿Para qué se usan?	El nombre completo, cargo e institución se usan para generar usuario, perfil y contraseña necesarios para el acceso a las herramientas de curación. El nombre completo, institución, puesto, correo electrónico institucional y teléfono institucional, se publican como metadatos asociados a registros de colecciones, en las secciones de datos curatoriales, datos de colecta y de contacto de la colección.	
Los datos se transfieren o se comparten	Si (X) No ( )	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal (X)	Gobierno Estatal (X) Gobierno Municipal (X) Personas físicas (X) Personas morales (X) Áreas Universitarias (X) Los datos de acceso (nombre completo, usuario, perfil y contraseña) son compartidos

		entre el personal autorizado dentro de la misma Área Universitaria, involucrado en el proceso. Los datos personales publicados como metadatos, son visibles en las fichas de ejemplares en el Portal de Datos Abiertos UNAM, Colecciones Universitarias y descargables mediante protocolos de interoperabilidad públicos.
¿Dónde se alojan?	[redacted]	
¿Cuánto tiempo se da tratamiento?	Herramientas de curación: Mientras el usuario siga activo en el sistema. Responsable de colecciones: Desde que los datos son cosechados hasta que el registro esté publicado en la	

	plataforma del Portal de Datos Abiertos UNAM, Colecciones Universitarias y mediante protocolos de interoperabilidad.
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Herramientas de curación: Recibir la solicitud, integrar los datos al archivo de usuarios, generar el usuario y contraseña, y entregar el oficio con los datos de ingreso. Contacto de la colección: Revisar que los datos personales contenidos en los metadatos se almacenen y accedan sin comprometer la integridad de los mismos.
Obligaciones:	Herramientas de curación: Atender la solicitud conforme al procedimiento correspondiente, generar el oficio cuando procede y resguardar los datos del usuario y su acceso en el archivo encriptado. Eliminar el correo de solicitud que contiene los datos personales de forma segura. Realizar todo el proceso sin comprometer la confidencialidad de los datos personales. Contacto de la colección: Recibir la solicitud de propagación de metadatos de la CDI. Supervisar la integración de los metadatos a las fuentes de datos que alimentan al Portal de Datos Abiertos UNAM, Colecciones Universitarias y a sus protocolos de interoperabilidad. Supervisar que todo el proceso se realice en bases de datos de acceso restringido, sin comprometer la integridad de los datos personales.

Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación
Funciones:	Herramientas de curación: Recibir la solicitud, verificar el perfil solicitado y autorizar la generación. Contacto de la colección: Revisar que los datos personales contenidos en los metadatos que describen los registros de colecciones se obtengan, registren, organicen, almacenen y accedan sin comprometer la integridad de los mismos.
Obligaciones:	Herramientas de curación: Revisar y autorizar la solicitud conforme al procedimiento correspondiente. Eliminar el correo de solicitud que contiene los datos personales de forma segura. Realizar el proceso sin comprometer la confidencialidad de los datos personales. Contacto de la colección: Supervisar el tratamiento de metadatos conforme al protocolo de integración de colecciones. Enviar la solicitud de propagación de datos a DTI. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Edurne Uriarte Santillán
Cargo:	Inventario de Colecciones y Datos de Investigación

Funciones:	Recabar, revisar, registrar, organizar, comunicar, almacenar y suprimir la información relativa a la gestión del personal.
Obligaciones:	Recibir oficio con datos de ingreso de la DTI, entregarlo al solicitante e ingresar al archivo el acuse de recibido. Recibir oficio y entregarlo al solicitante, resguardando en el archivo el acuse.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Encargado	
Nombre:	Cecelic Reséndiz Arias
Cargo:	No aplica
Funciones:	Obtener, registrar, organizar y almacenar los datos personales contenidos en los metadatos que describen las Colecciones y aquellos para definir un perfil de usuario, sin comprometer la integridad de los mismos.
Obligaciones:	Herramientas de curación: Revisar el perfil del usuario para indicarlo a DTI. Contacto de la colección: Realizar los procesos involucrados en la integración de colecciones conforme al protocolo correspondiente.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Encargado	
Nombre:	Efraín Hipólito Chamú
Cargo:	No aplica
Funciones:	Obtener, registrar, organizar y almacenar los datos personales contenidos en los

	metadatos que describen las Colecciones sin comprometer la integridad de los mismos.
Obligaciones:	Contacto de la colección: Realiza la cosecha de datos y organiza la información para el proceso de integración al esquema del Portal de Datos Abiertos UNAM, Colecciones Universitarias. Ejecuta el proceso de propagación hacia las fuentes de datos que alimentan a la plataforma del Portal de Datos Abiertos UNAM, Colecciones Universitarias. Realizar todo el proceso en bases de datos de acceso restringido, sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Encargado	
Nombre:	Alejandro Chávez Méndez
Cargo:	No aplica
Funciones:	Resguardar de manera segura los datos personales contenidos en los documentos físicos y digitales relacionados con el proceso de las herramientas de curación.
Obligaciones:	Seguir el procedimiento para un resguardo seguro del documento. Resguardar los documentos relacionados con la DGRU. Digitalizar los documentos que contienen los datos personales, asegurando la integridad de dichos datos personales. Archivar el documento digital en un espacio encriptado en la DGRU. Archivar el documento físico conforme a los Instrumentos de Control y Consulta Archivística de la UNAM. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Usuarios	
Nombre:	No aplica

Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

8.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Coordinación de Colecciones y Datos de Investigación, DGRU	
Identificador único	CDI1
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias
Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]

[redacted]

8.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Bases de datos que pueden contener información personal y oficios con datos de acceso.	Los metadatos de los registros de colecciones son primordiales pues se publican en el Portal de Datos Abiertos UNAM, Colecciones Universitarias, siendo éste una de las plataformas principales desarrolladas y administradas por la DGRU. Los datos personales asociados a los registros de colecciones, resultan esenciales para propósitos de identificación, mientras que aquellos utilizados para la elaboración de datos de acceso, son necesarios para labores de revisión de la información.	Bases de datos de registros de colecciones que posiblemente contengan datos personales de identificación y oficios con información laboral para asignar claves de acceso a las herramientas de curación de la plataforma digital.
Dueño		
¿A quién pertenece el activo de información?		
Coordinador de Colecciones y Datos de Investigación		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	Los datos de acceso a la plataforma se considerarán confidenciales y únicamente personal autorizado podrá

		acceder a ellos.
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente manera:	La información únicamente podrá ser modificada por personal autorizado de la DGRU.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera:	La información laboral para la generación de datos de acceso debe estar disponible para que el personal asignado realice las actividades.
	Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	Los metadatos asociados a las colecciones digitales publicadas en el PDA deberán estar disponibles para su consulta.
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
( ) Confidencialidad	**(X) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	
[redacted]	

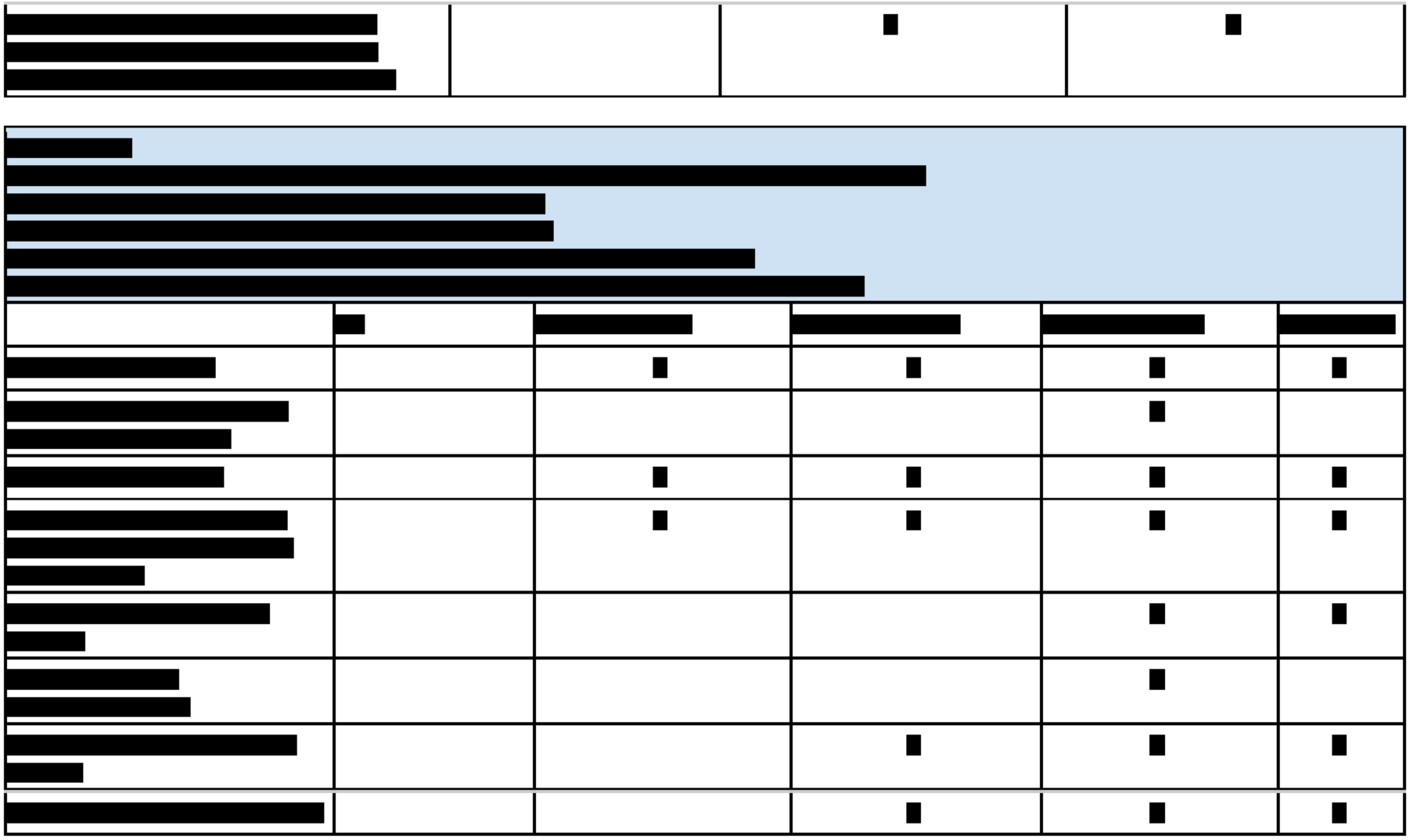
8.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Portal de Datos Abiertos UNAM, Colecciones Universitarias
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]



[redacted]					

CONTENEDORES FÍSICOS

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]			
[redacted]			

[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

[redacted]

	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]
[redacted]		[redacted]	[redacted]	[redacted]	[redacted]

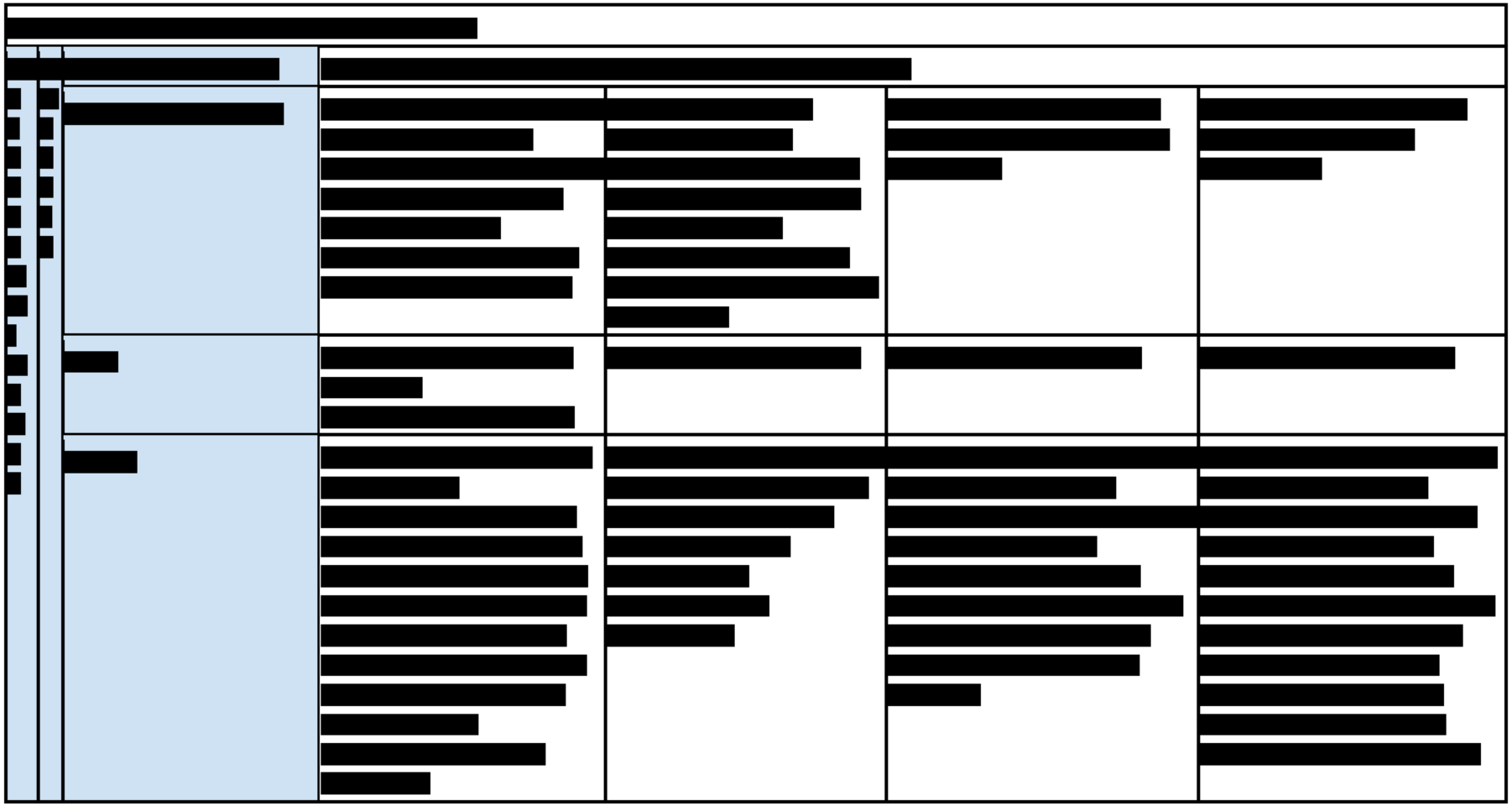
RECURSOS HUMANOS

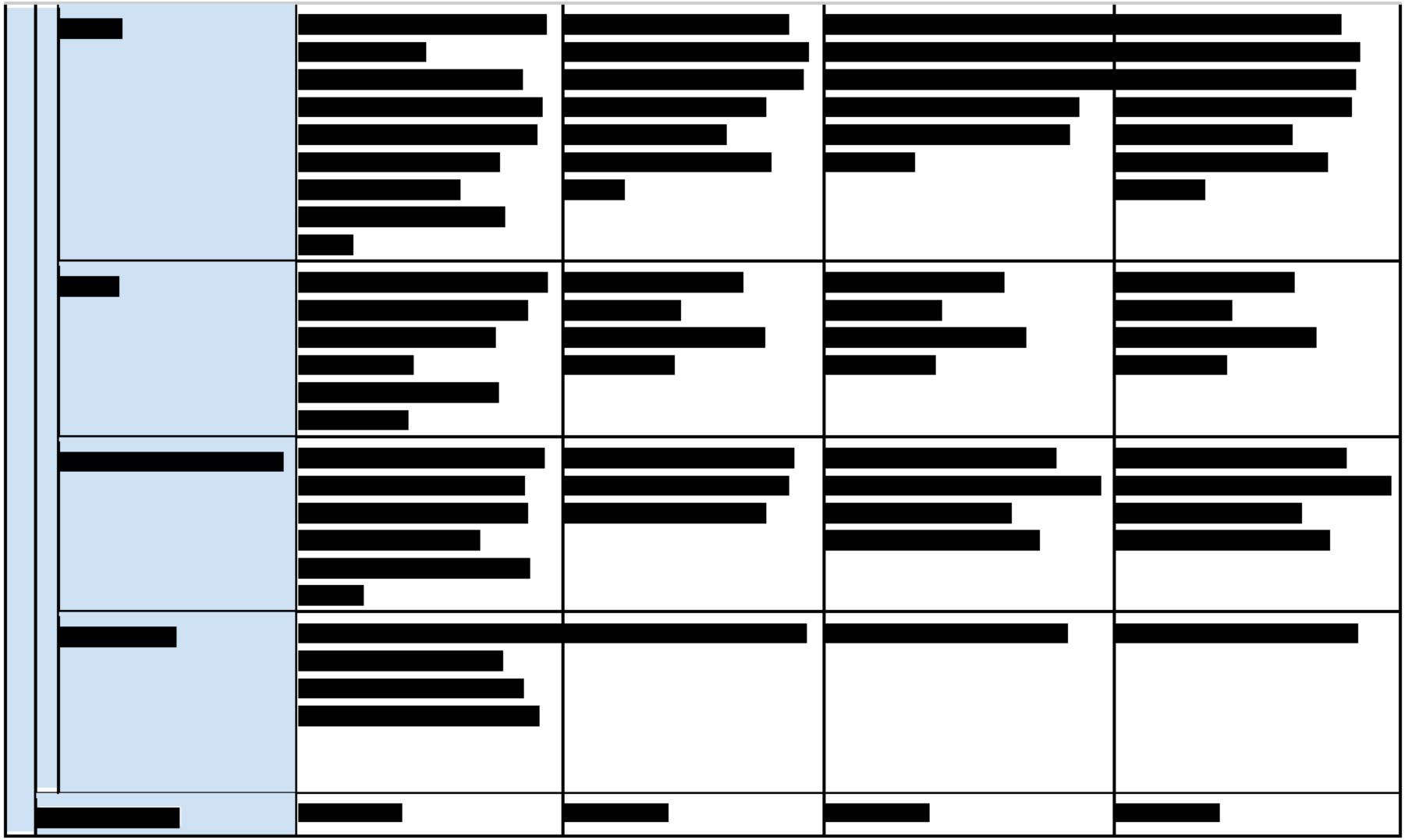
[redacted]

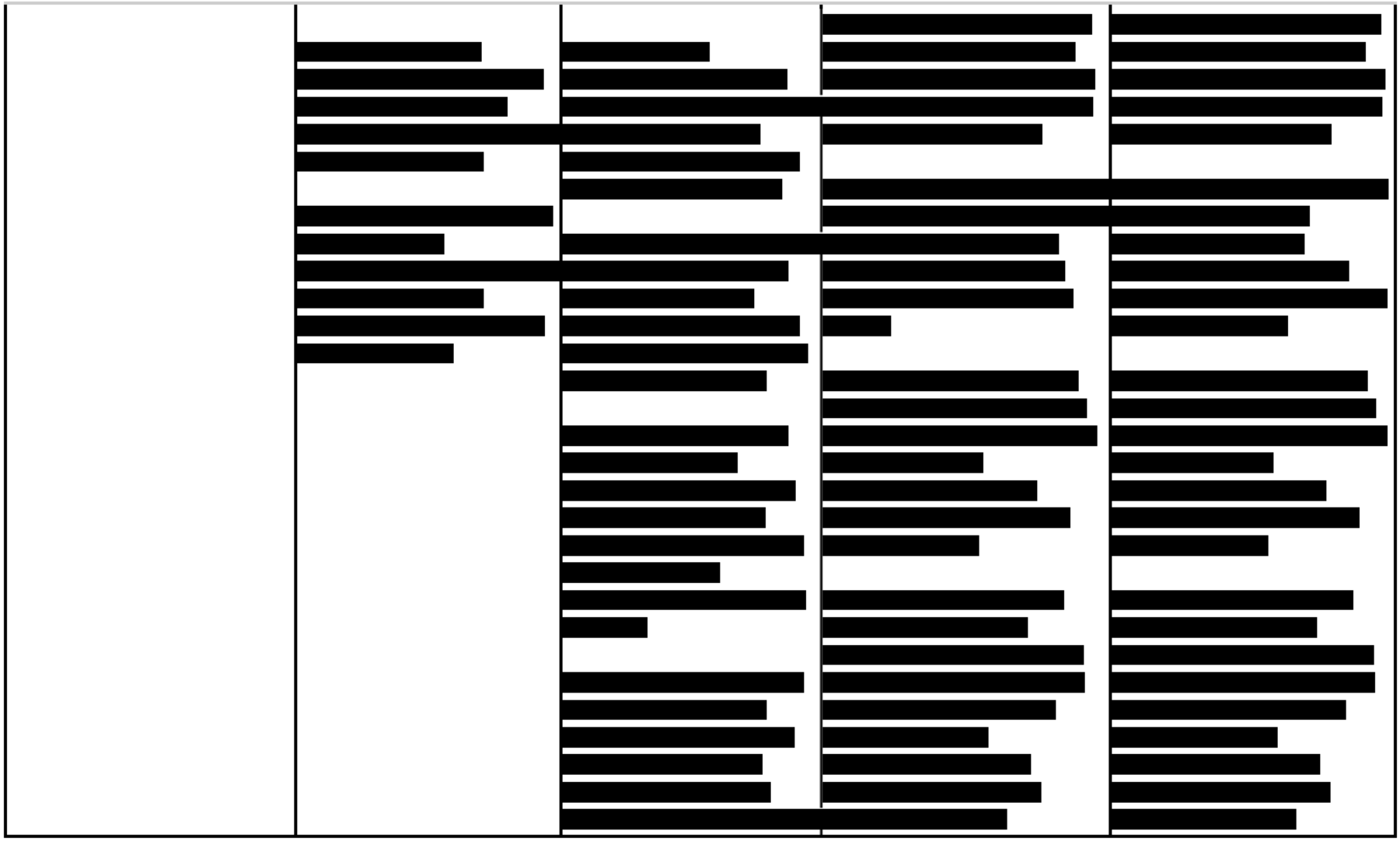
[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

8.5. ANÁLISIS DE RIESGOS





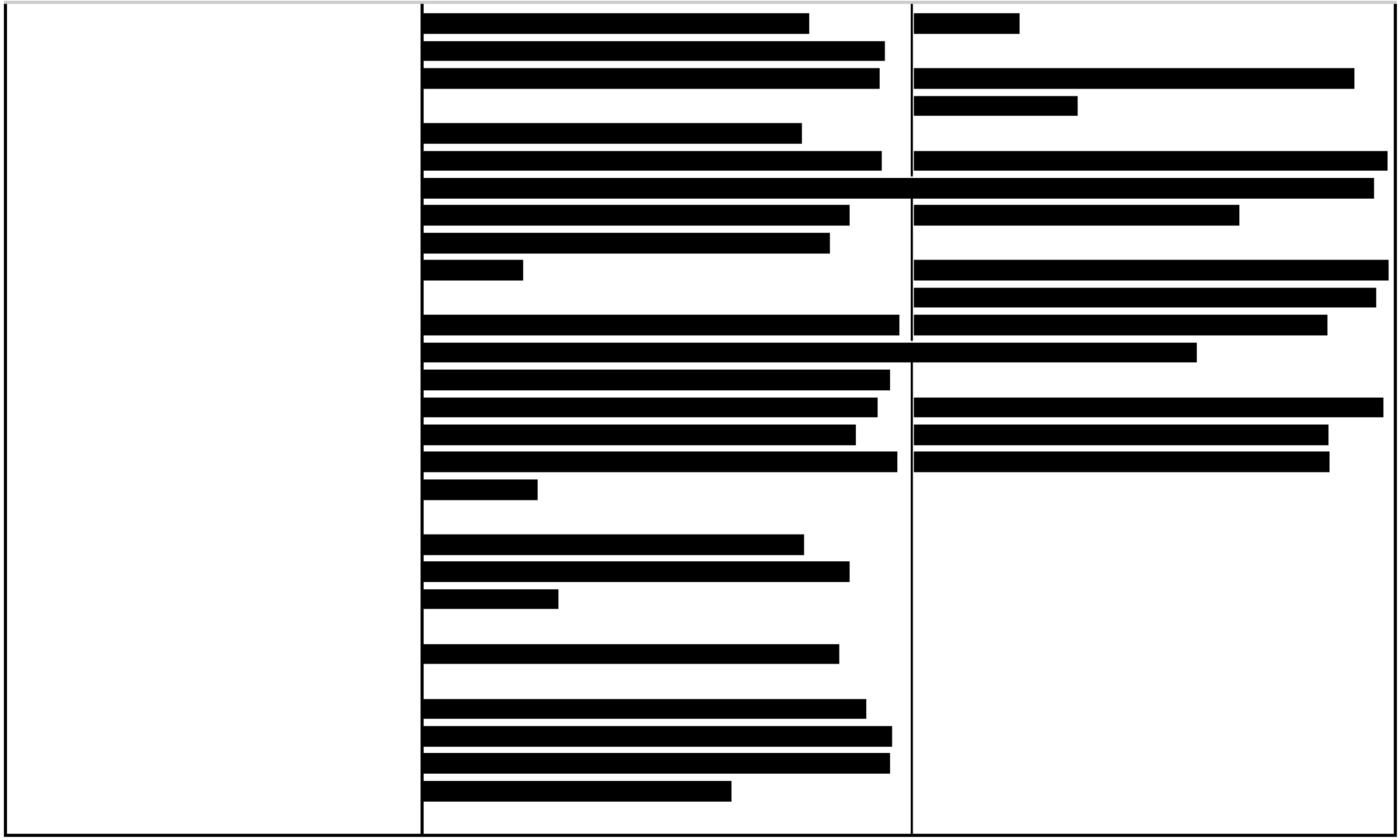


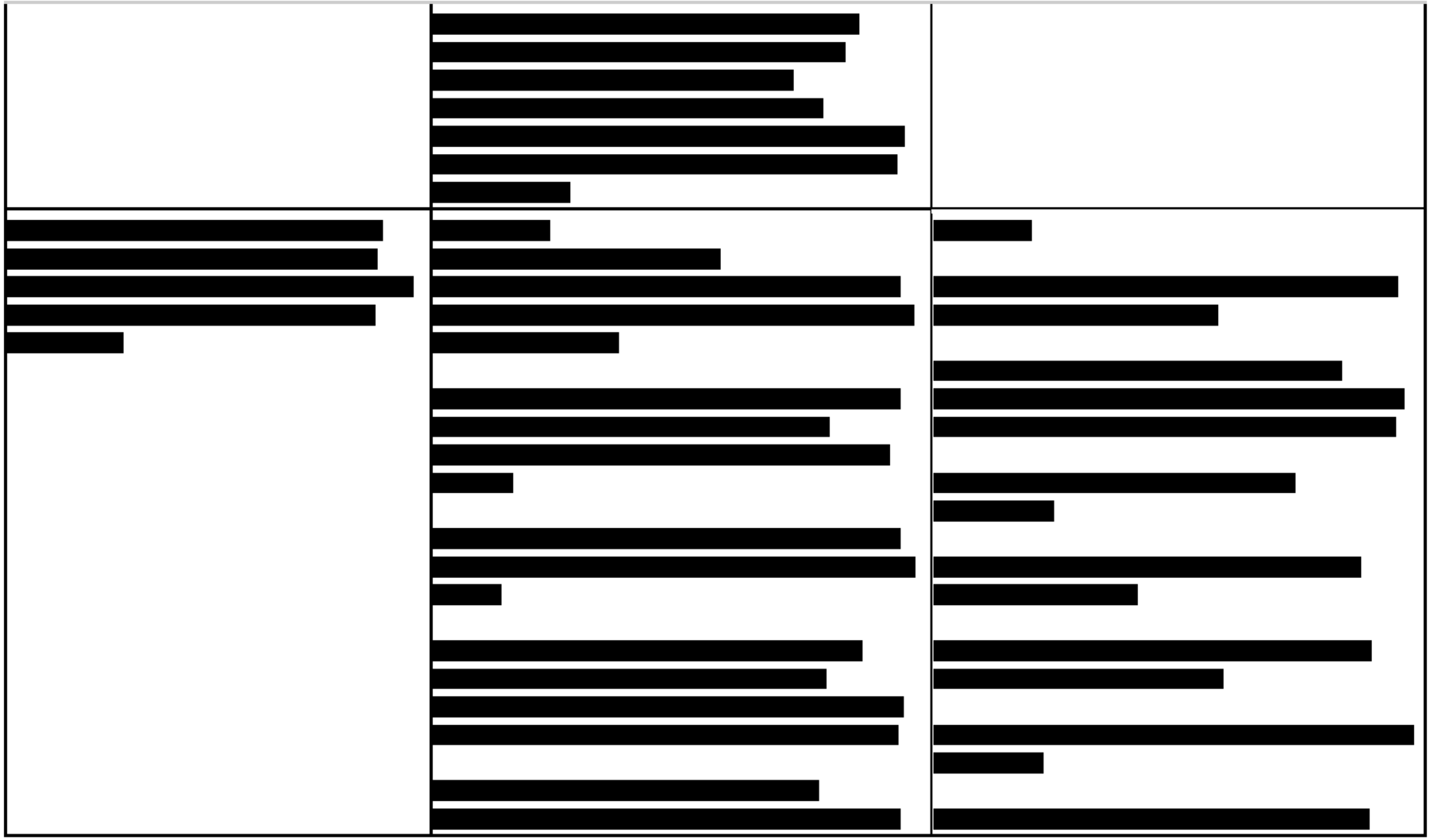
		[redacted]	[redacted]	[redacted]

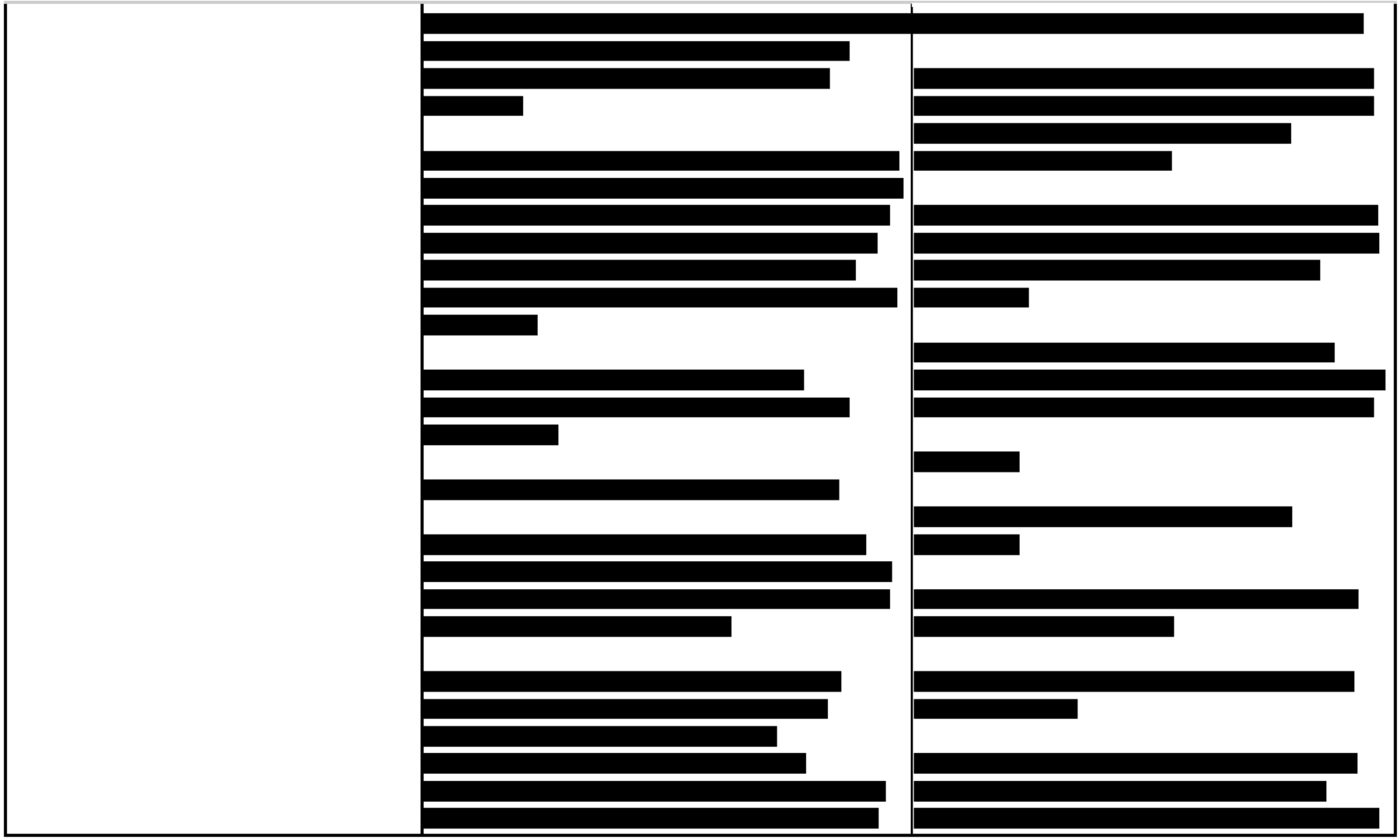
Coordinación de Colecciones y Datos de Investigación, DGRU	
Identificador único	CDI1
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias

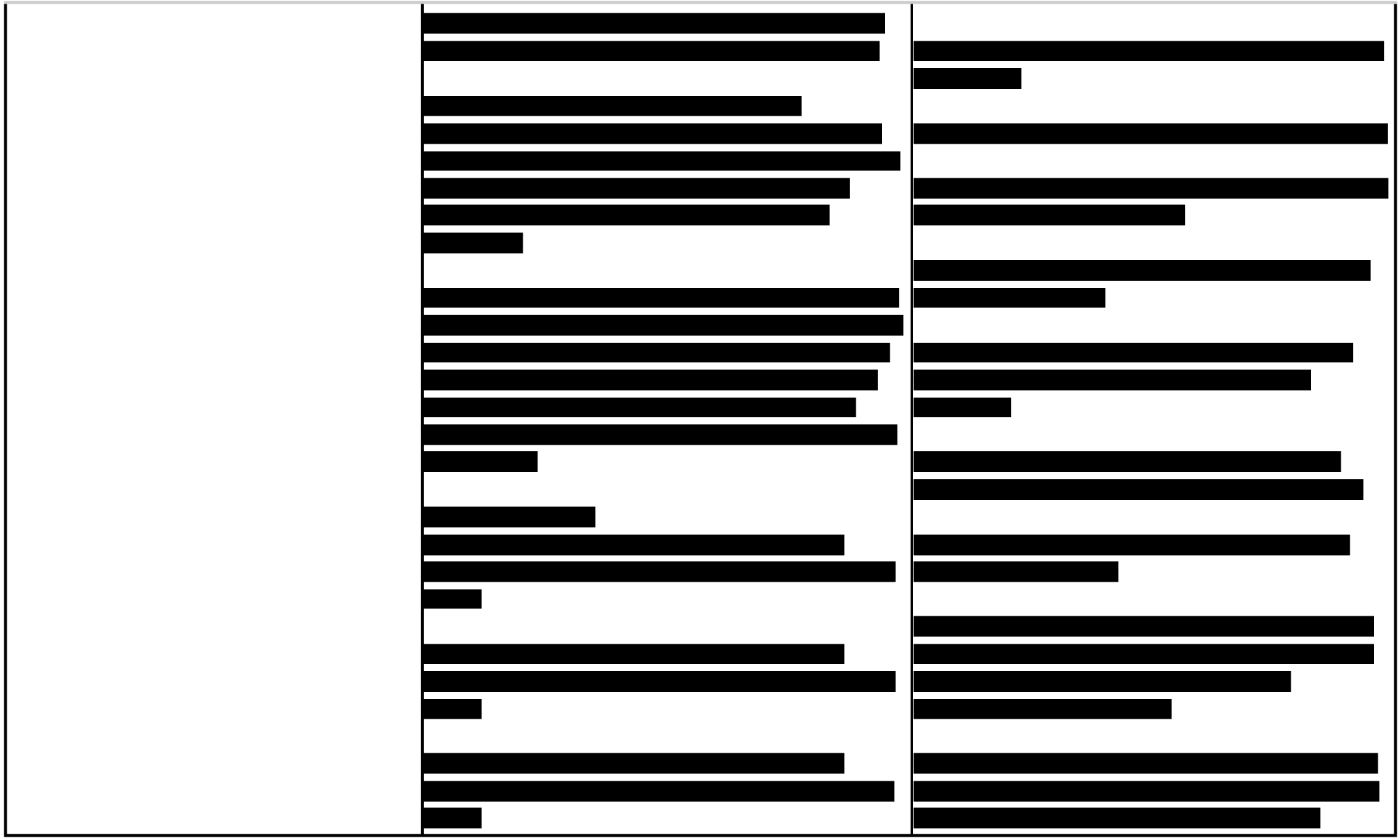
ANÁLISIS DE RIESGOS

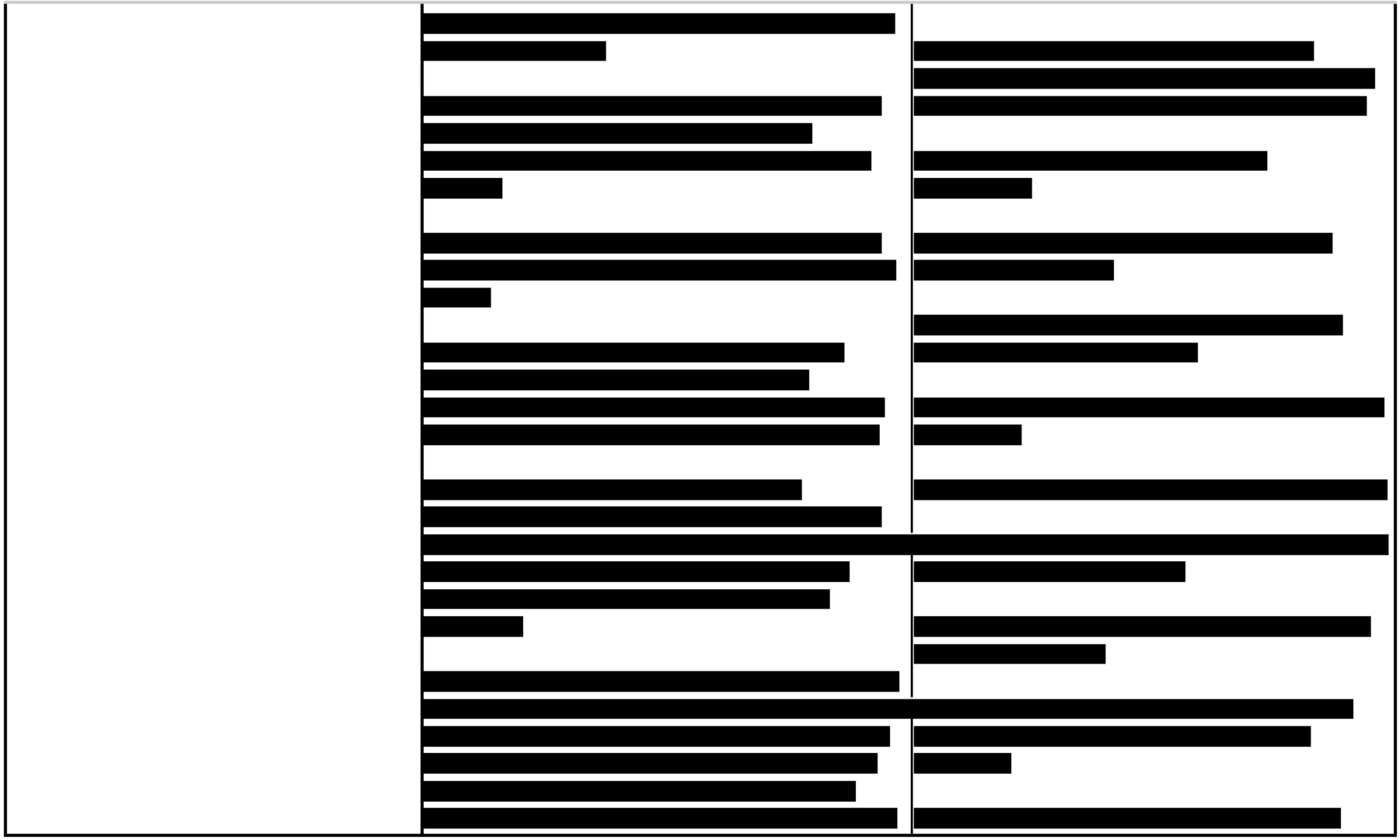
Riesgo	Impacto	Mitigación
[redacted]	[redacted]	[redacted]

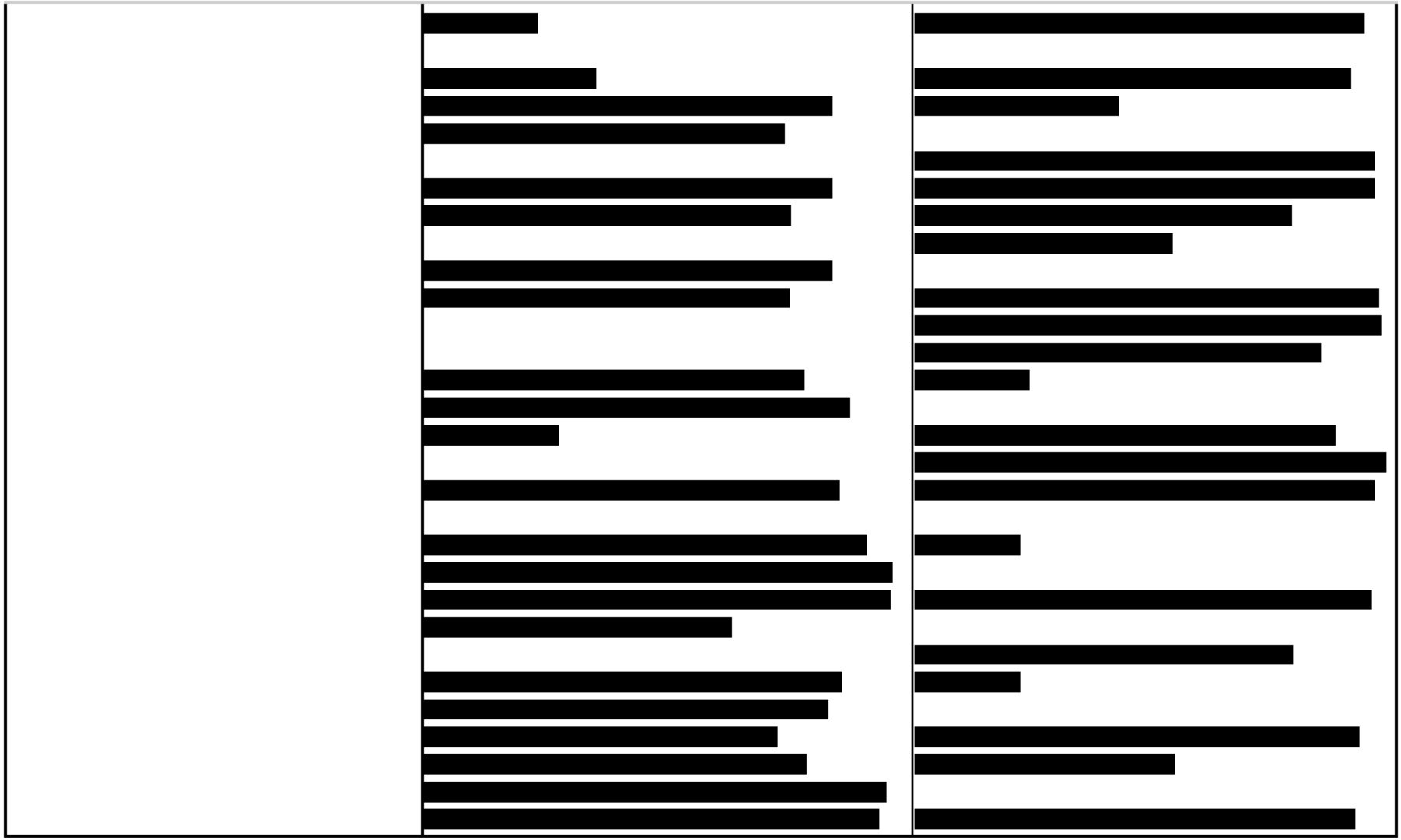












	[redacted]	[redacted]

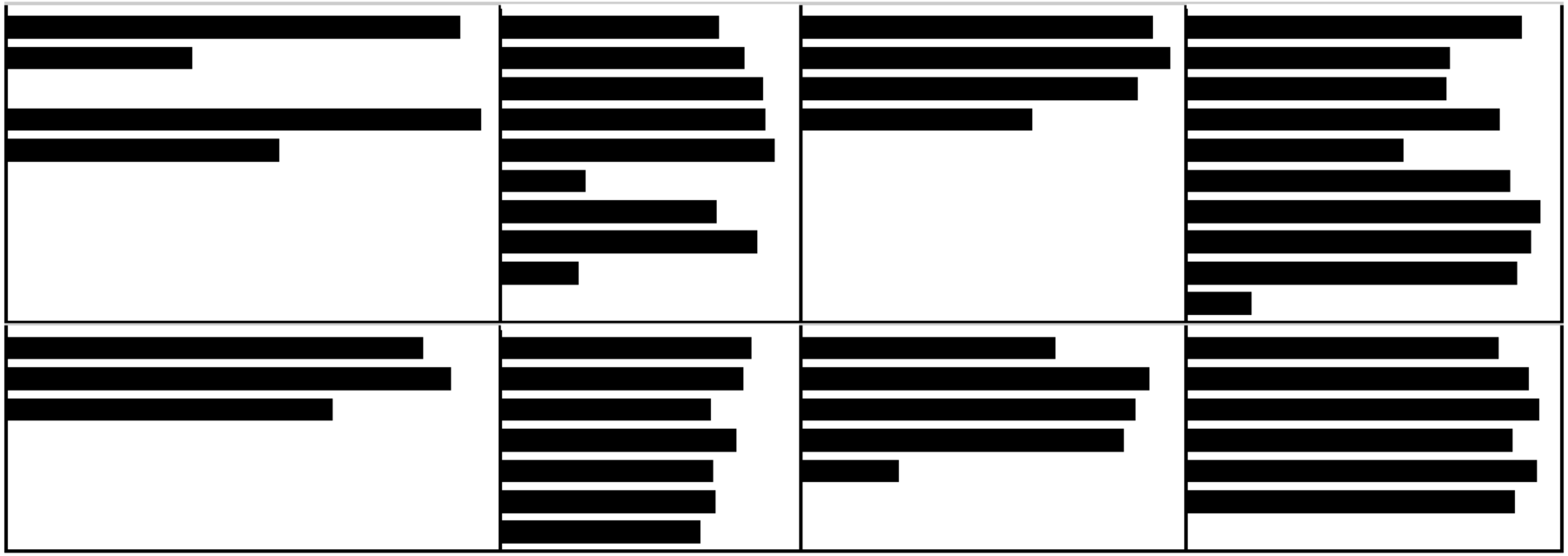
8.6. ANÁLISIS DE BRECHA

Coordinación de Colecciones y Datos de Investigación, DGRU			
Identificador único	CDI1		
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]			
[redacted]			
[redacted]			

[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	

[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			



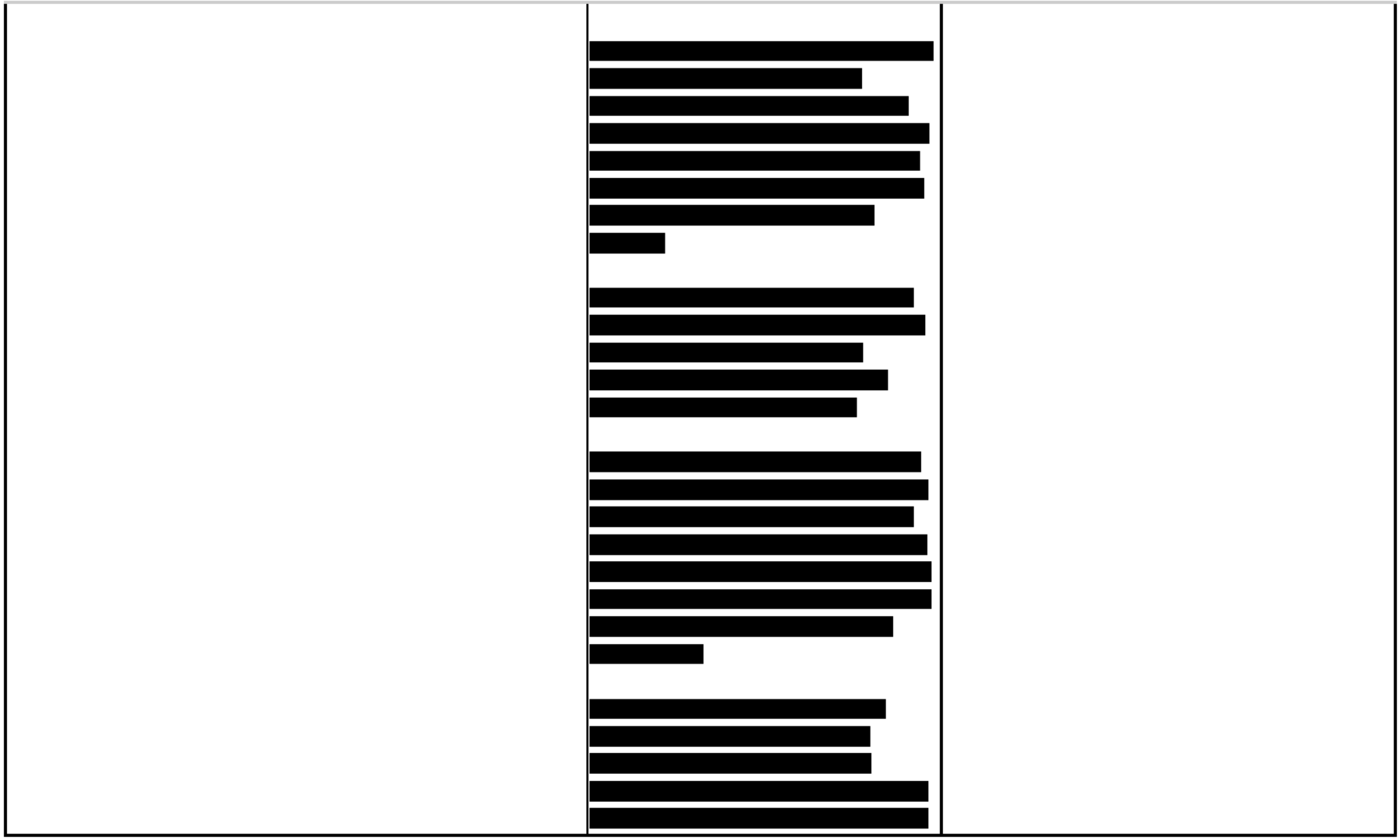
8.7. PLAN DE TRABAJO

Coordinación de Colecciones y Datos de Investigación, DGRU				
Identificador único	CDI1			
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]			

8.8. MEDIDAS DE SEGURIDAD

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

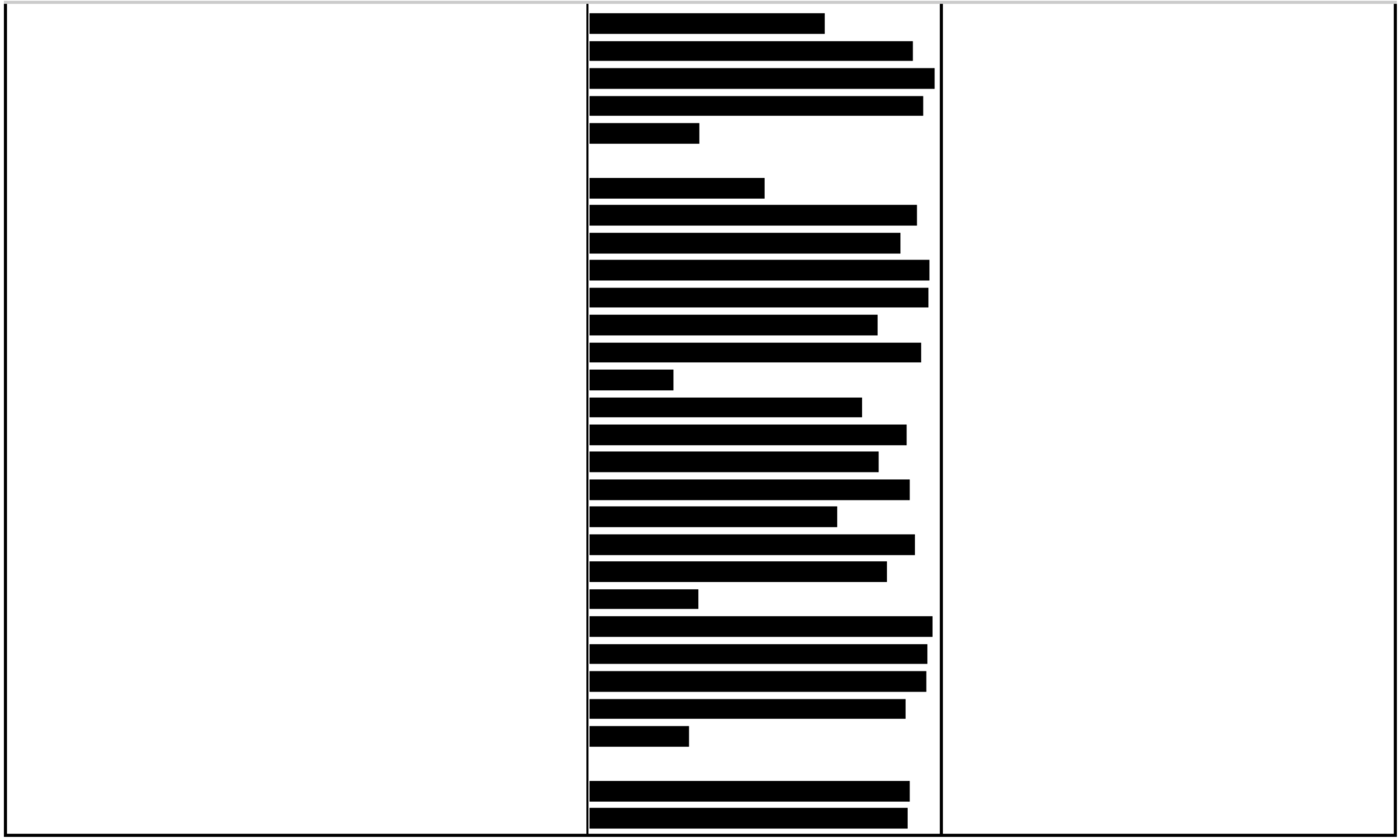


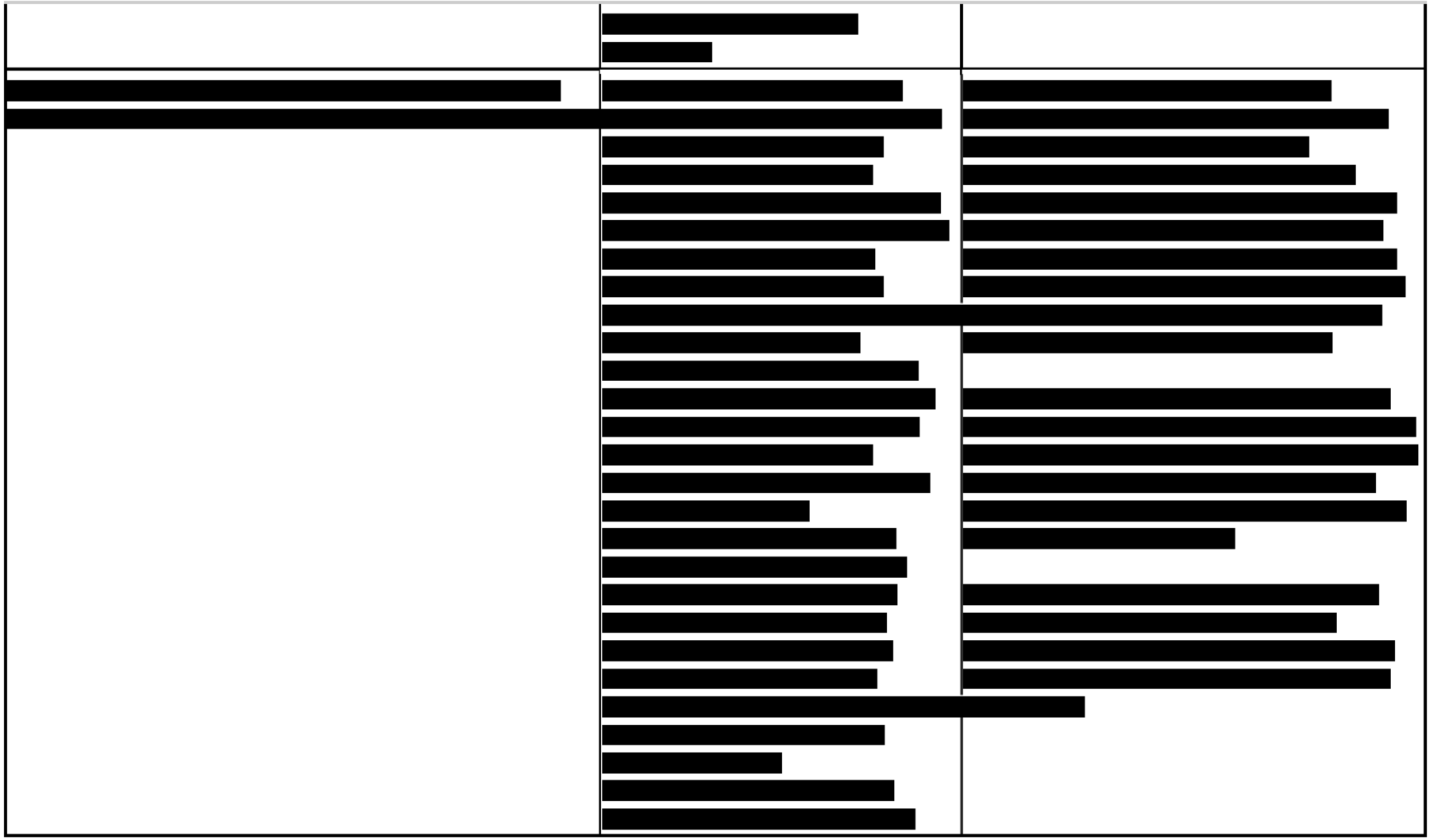
	[redacted]	

Coordinación de Colecciones y Datos de Investigación, DGRU	
Identificador único	CDI1
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	

[redacted]

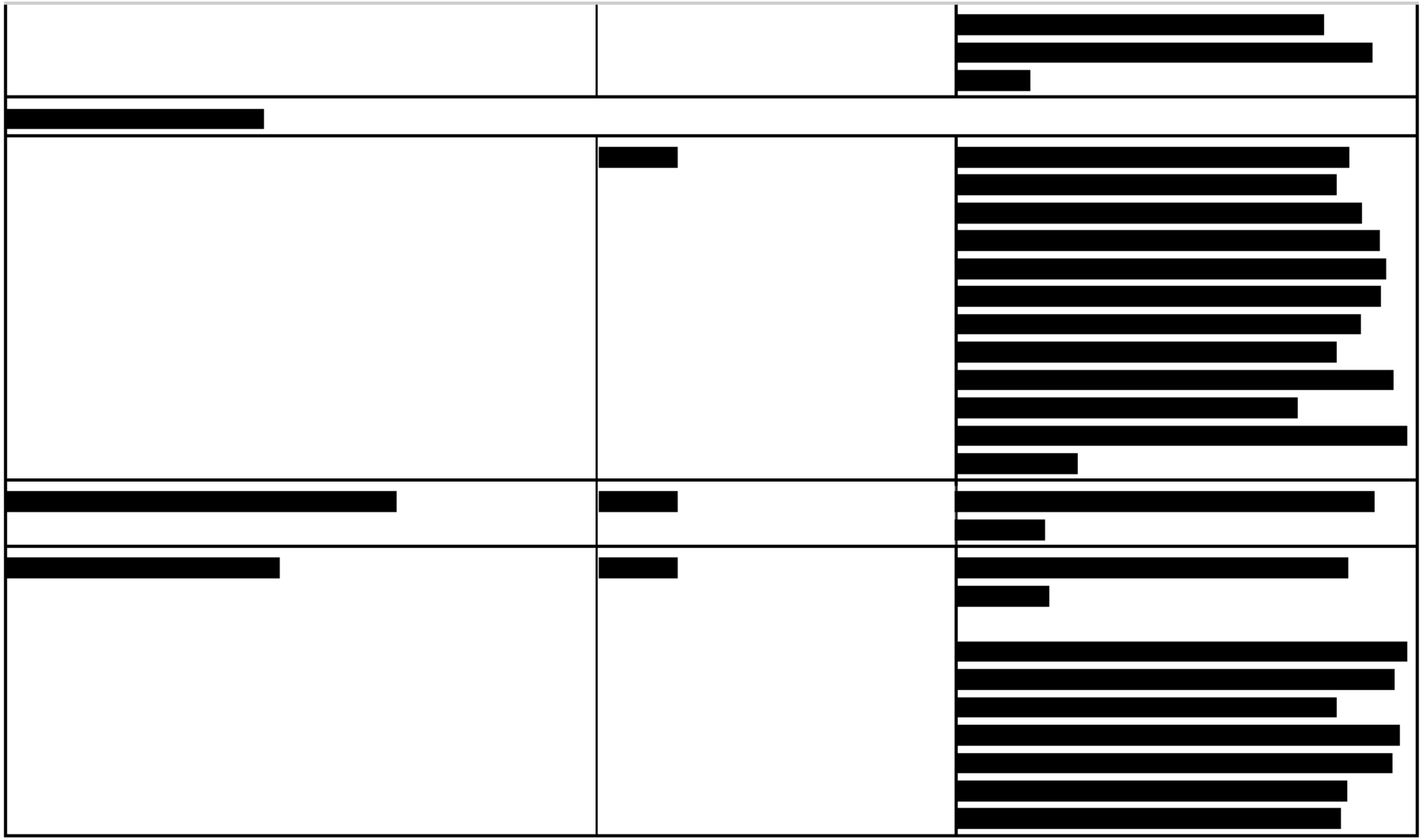
Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]

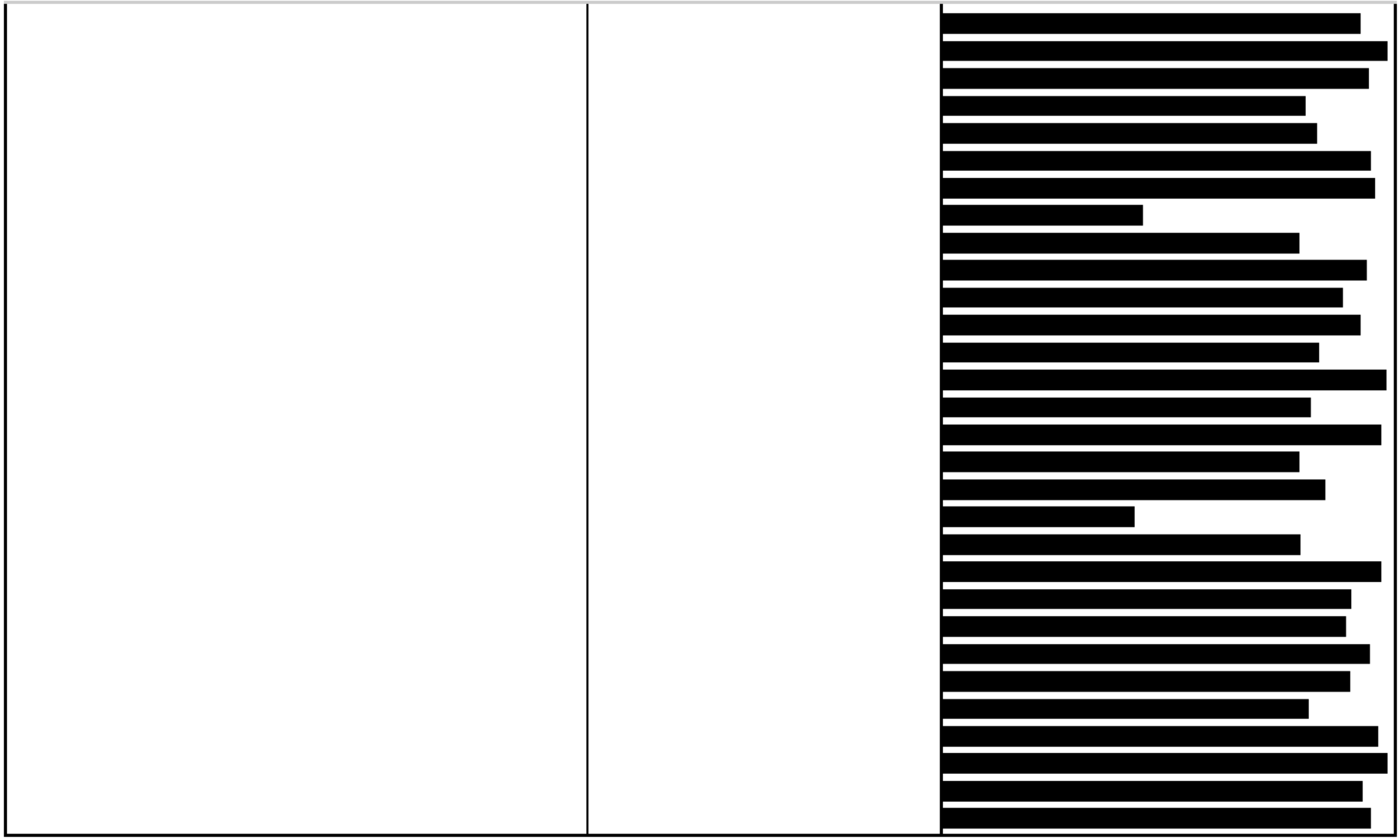




[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
	[redacted]	[redacted]

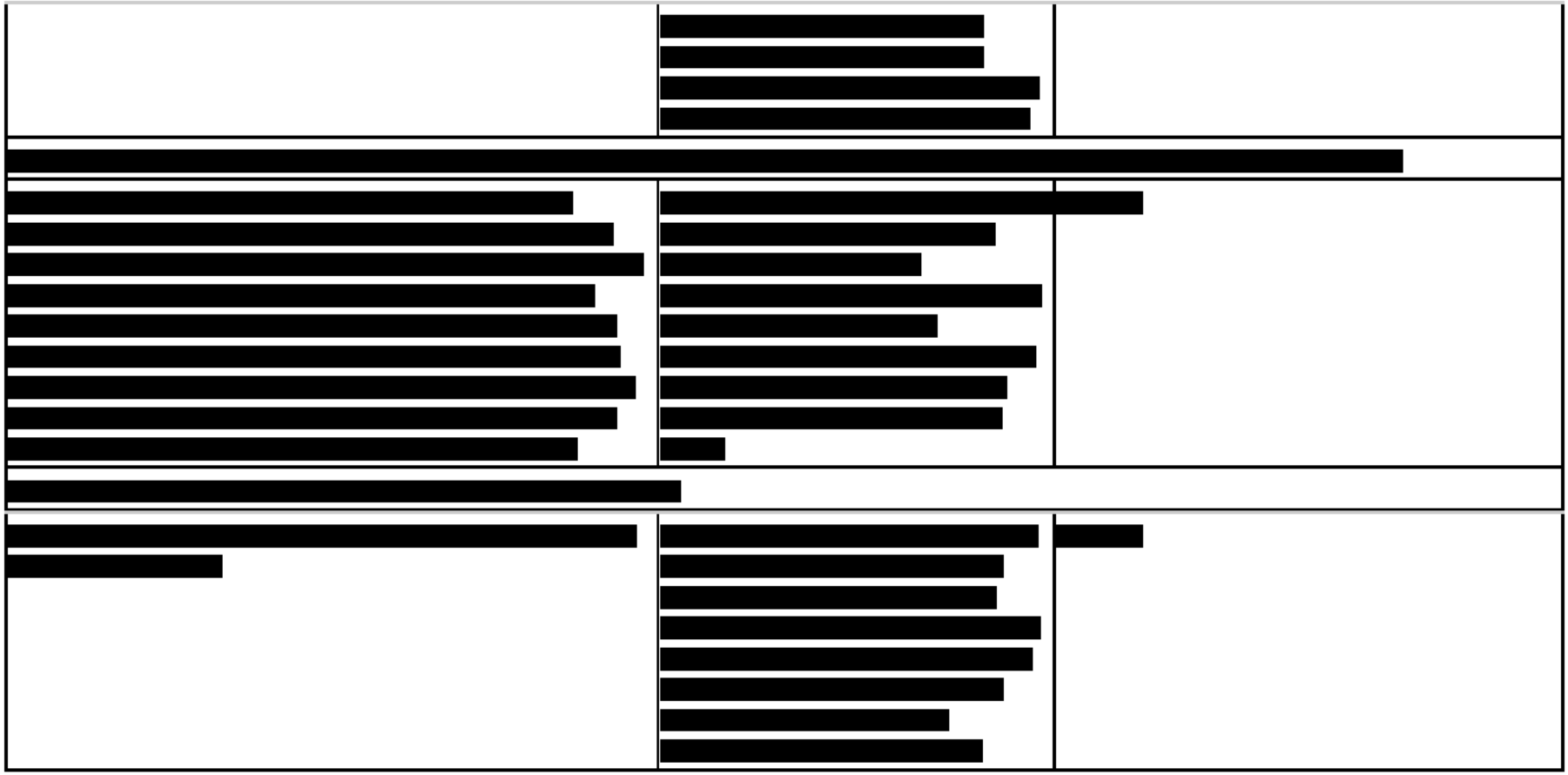




		por teléfono.
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		

	[redacted]	[redacted]

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	
[redacted]		
[redacted]	[redacted]	



Coordinación de Colecciones y Datos de Investigación, DGRU	
Identificador único	CDI1

Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

8.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Coordinación de Colecciones y Datos de Investigación, DGRU

Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
Recurso	Descripción	Control
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
Medida de seguridad	Procedimiento	Responsable
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Coordinación de Colecciones y Datos de Investigación, DGRU		
Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Coordinación de Colecciones y Datos de Investigación, DGRU

Identificador único	CDI1	
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias	
Medida de seguridad	Acciones	Responsable
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

8.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Coordinación de Colecciones y Datos de Investigación, DGRU				
Identificador único	CDI1			
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias			
Actividad	Descripción	Duración	Cobertura	Prioridad
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales.	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Coordinación de Colecciones y Datos de Investigación, DGRU				
Identificador único	CDI1			
Nombre del sistema CDI1	Portal de Datos Abiertos UNAM, Colecciones Universitarias			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales. - Procedimientos de borrado seguro de correos electrónicos y de archivos.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones de Colecciones y Datos de Investigación, Desarrollo Tecnológico e Infraestructura y de Planeación, Gestión y Normatividad involucrado en la operación del Portal de Datos Abiertos UNAM.	Alta

- Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Uso adecuado de datos personales durante el desarrollo involucrado en las bases de datos que los contienen. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.			Frecuencia de la actualización una vez al año o antes si se considera necesario.	

Anexo 9. DTI1 Correo electrónico

9.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI1
Nombre del sistema DTI1	Correo electrónico
Datos personales (sensible o no) contenidos en el sistema:	1 Datos personales en general: 1a. Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, fotografía, idioma o lengua. 1b. Datos laborales: Documentos de reclutamiento y selección, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales. 1c. Datos patrimoniales: información fiscal, ingresos, cuentas bancarias. 1d. Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales: Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia penal, administrativa, con independencia de su etapa de trámite. 1e. Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos.
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X)
¿Para qué se usan?	Los datos señalados se usan en comunicaciones para el apoyo en la gestión de procesos internos y el ejercicio de las actividades sustantivas de la DGRU. La comunicación puede ser a través de las cuentas de correo electrónico: contacto@dgru.unam.mx, archivo@dgru.unam.mx, ayuda@dgru.unam.mx, contacto@repositorio.unam.mx y todas las cuentas institucionales del personal que labora para la DGRU con dominio @dgru.unam.mx o @ccud.unam.mx.
Los datos se transfieren o se comparten	Si (X) No ( )

	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal (X) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas físicas (X) Personas morales ( ) Áreas Universitarias (X)	Los datos personales se comparten con personal interno, otras áreas universitarias, externas a la Universidad, o personas físicas, según el caso particular que se trate, cuando sea indispensable para el desempeño de las funciones de la DGRU.
¿Dónde se alojan?	[redacted]	
¿Cuánto tiempo se da tratamiento?	Los correos electrónicos pueden conservarse hasta un año o hasta que el proceso de gestión concluya. La disposición de documentos es el establecido en los Instrumentos de Control y Consulta Archivística de la UNAM vigentes.	
Responsable		
Nombre:	Tila María Pérez Ortiz	
Cargo:	Directora General de Repositorios Universitarios	
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.	
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las	

	medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Responsable	
Nombre:	Ariana Chávez Méndez
Cargo:	Coordinadora de Planeación, Gestión y Normatividad
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Oliver Joaquín Giménez Héau
Cargo:	Coordinador de Colecciones y Datos de Investigación

Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Rubén Ignacio Sáenz González
Cargo:	Coordinador del Sistema de Repositorios Universitarios
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Dirección General
Responsable	
Nombre:	Ana Laura Méndez Franco
Cargo:	Jefa de Departamento de Planeación y Seguimiento de Proyectos
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida. Resguardar de manera segura los correos electrónicos que le sean indicados y/o los documentos adjuntos.
Obligaciones:	Indicar en qué expediente de archivo se deben resguardar los correos electrónicos, y en su

	caso los documentos adjuntos, enviarlos a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Responsable	
Nombre:	Edurne Dolores Uriarte Santillán
Cargo:	Jefa de Departamento de Inventario de Colecciones y Datos de Investigación
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General
Responsable	
Nombre:	Daniel Pérez Castillo
Cargo:	Jefe de Departamento de Datos de Investigación
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Coordinador de Colecciones y Datos de Investigación y Dirección General

Responsable	
Nombre:	Roberto Rico Chávez
Cargo:	Jefe de Departamento de Infraestructura, Centro de Datos y Servicios
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Responsable	
Nombre:	Oscar Hernández Hernández
Cargo:	Jefe de Departamento de Instalación y Soporte de Repositorios Universitarios
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Coordinador de Sistema de Repositorios Universitarios y Dirección General
Responsable	
Nombre:	Areli Plancarte Salas
Cargo:	Asistente Ejecutivo
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y

	confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Coordinador del Sistema de Repositorios Universitarios y Dirección General
Encargado	
Nombre:	José Antonio Contreras Morales
Cargo:	Encargado de gestión administrativa
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Dirección General
Encargado	
Nombre:	Alejandro Chávez Méndez
Cargo:	No aplica
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida. Resguardar de manera segura los correos electrónicos que le sean indicados y/o los documentos adjuntos.
Obligaciones:	Seguir el procedimiento para un resguardo seguro de correos electrónicos. Archivar el correo electrónico y/o los documentos adjuntos, en un espacio encriptado en la

	DGRU y de conformidad con los Instrumentos de Control y Consulta Archivística de la UNAM. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas. Realizar el proceso sin comprometer la integridad de los datos personales.
Rinde cuentas a:	Coordinadora de Planeación, Gestión y Normatividad y Dirección General
Encargado	
Nombre:	Personal de servicios profesionales
Cargo:	No aplica
Funciones:	Dar seguimiento al asunto que involucra datos personales asegurando la integridad y confidencialidad de la información recibida, según corresponda a la tarea encomendada por el personal que lo supervisa.
Obligaciones:	En caso de que aplique, comunicar el correo a otras áreas internas de la DGRU y enviar a resguardo en Sistema Documental de la DGRU. Realizar el proceso sin comprometer la integridad de los datos personales, observando las medidas de tratamiento seguro de datos personales en comunicaciones electrónicas.
Rinde cuentas a:	Persona a cargo de la coordinación en que colabore y Dirección General

9.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI1
Nombre del sistema DTI1	Correo electrónico
Tipo de soporte:	[redacted]
Descripción:	[redacted]

	[redacted]
[redacted]	[redacted]

[redacted]

9.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	¿Por qué es importante el activo de información para la organización?	¿Cuál es la descripción condensada del activo de información?
Correos electrónicos con datos personales	Porque se intercambian datos personales o documentos recabados que son indispensables para llevar el desempeño de las funciones de la DGRU.	Los correos electrónicos pueden contener datos personales de identificación, laborales o académicos,.
Dueño		
¿A quién pertenece el activo de información?		
Propietarios de las cuentas de correo electrónico y personal asignado para atender: contacto@dgru.unam.mx, archivo@dgru.unam.mx, ayuda@dgru.unam.mx y contacto@repositorio.unam.mx		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	El personal que reciba un correo que contenga información personal será responsable de compartir los datos personales exclusivamente con destinatarios autorizados para el proceso que se trate.
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente	El personal que reciba un

	manera:	correo que contenga información personal es responsable de no alterar los datos personales recibidos y de comunicarlos cuando sea indispensable.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera: Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	La información contenida en los correos descritos debe estar disponible para que el personal autorizado realice las actividades asignadas.
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
(X) Confidencialidad	**( ) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	[redacted]
EXTERNO	

DESCRIPCIÓN DE CONTENEDOR	DUEÑO(S)
[redacted]	
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	[redacted]
EXTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**DUEÑO(S)**
[redacted]	
[redacted]	
[redacted]	

9.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Correo electrónico
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

CONTENEDORES TÉCNICOS

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

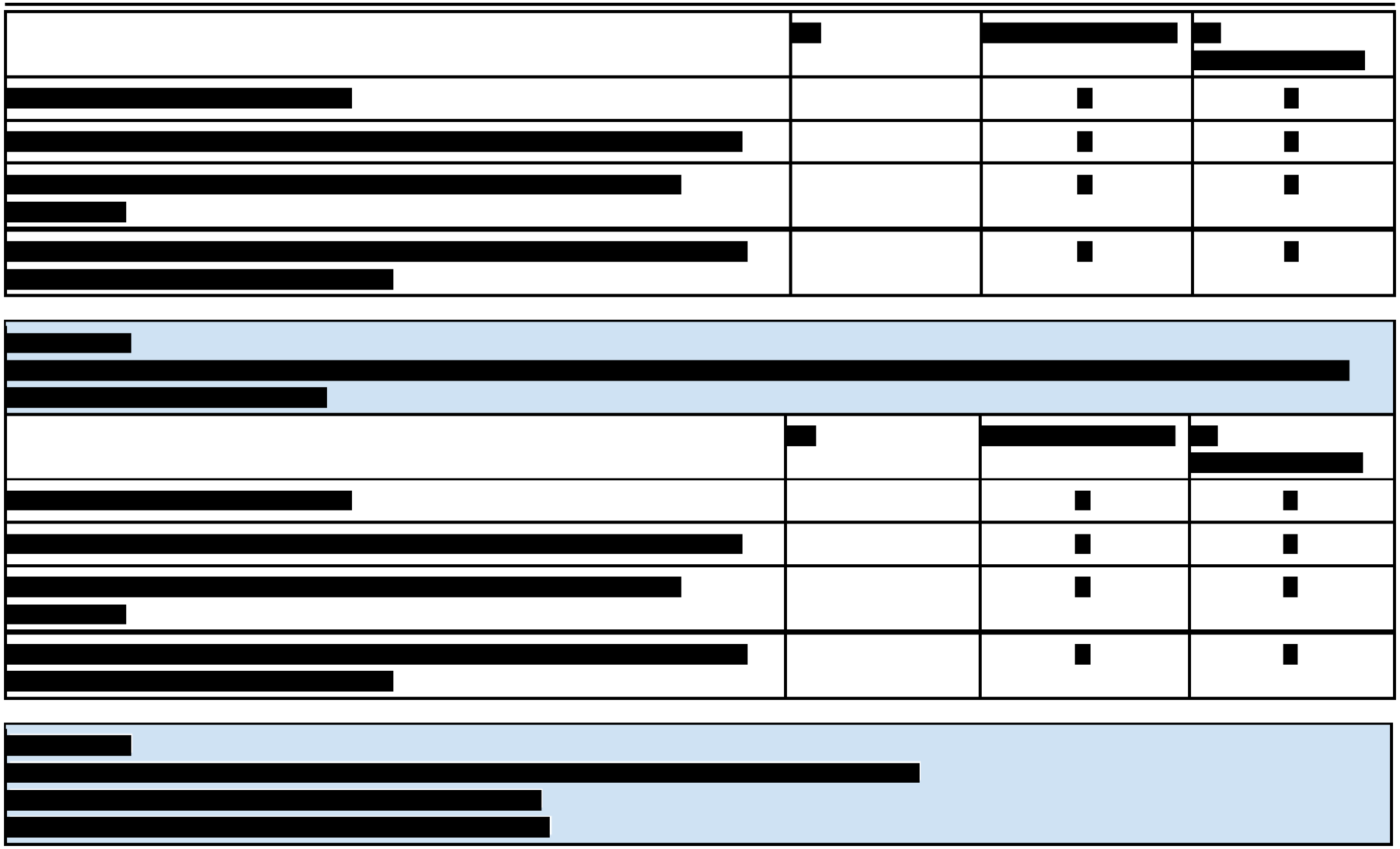
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]

[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					
[redacted]					

CONTENEDORES FÍSICOS

[redacted]



[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]					
[redacted]					

RECURSOS HUMANOS

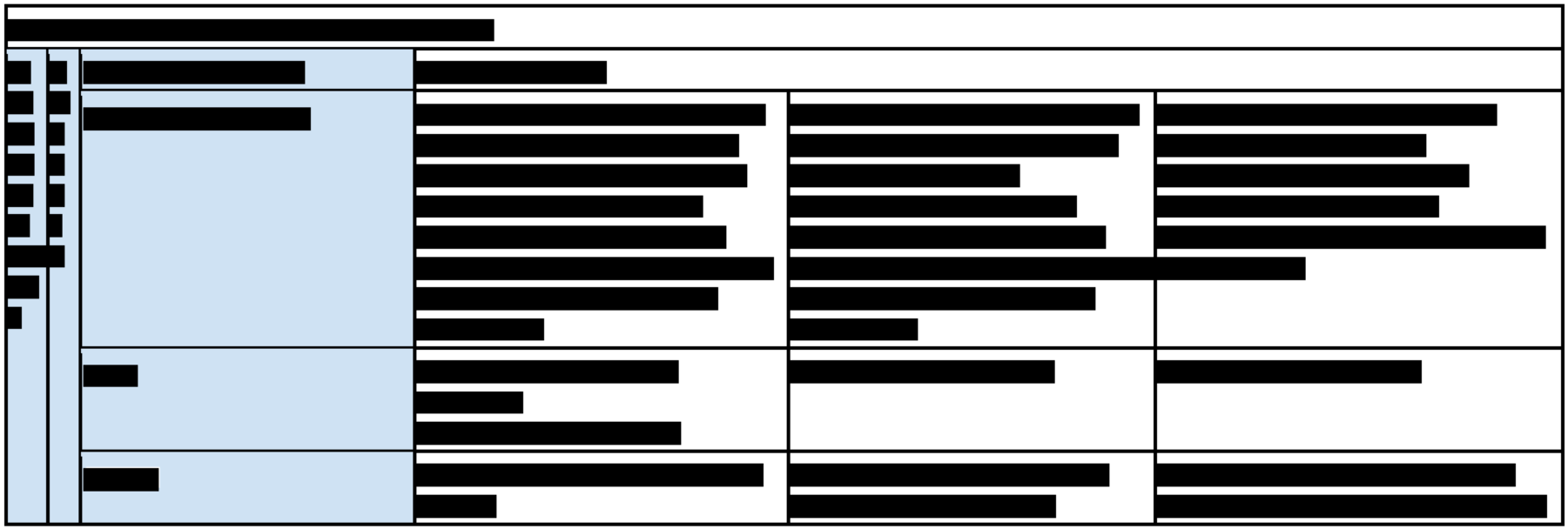
[redacted]

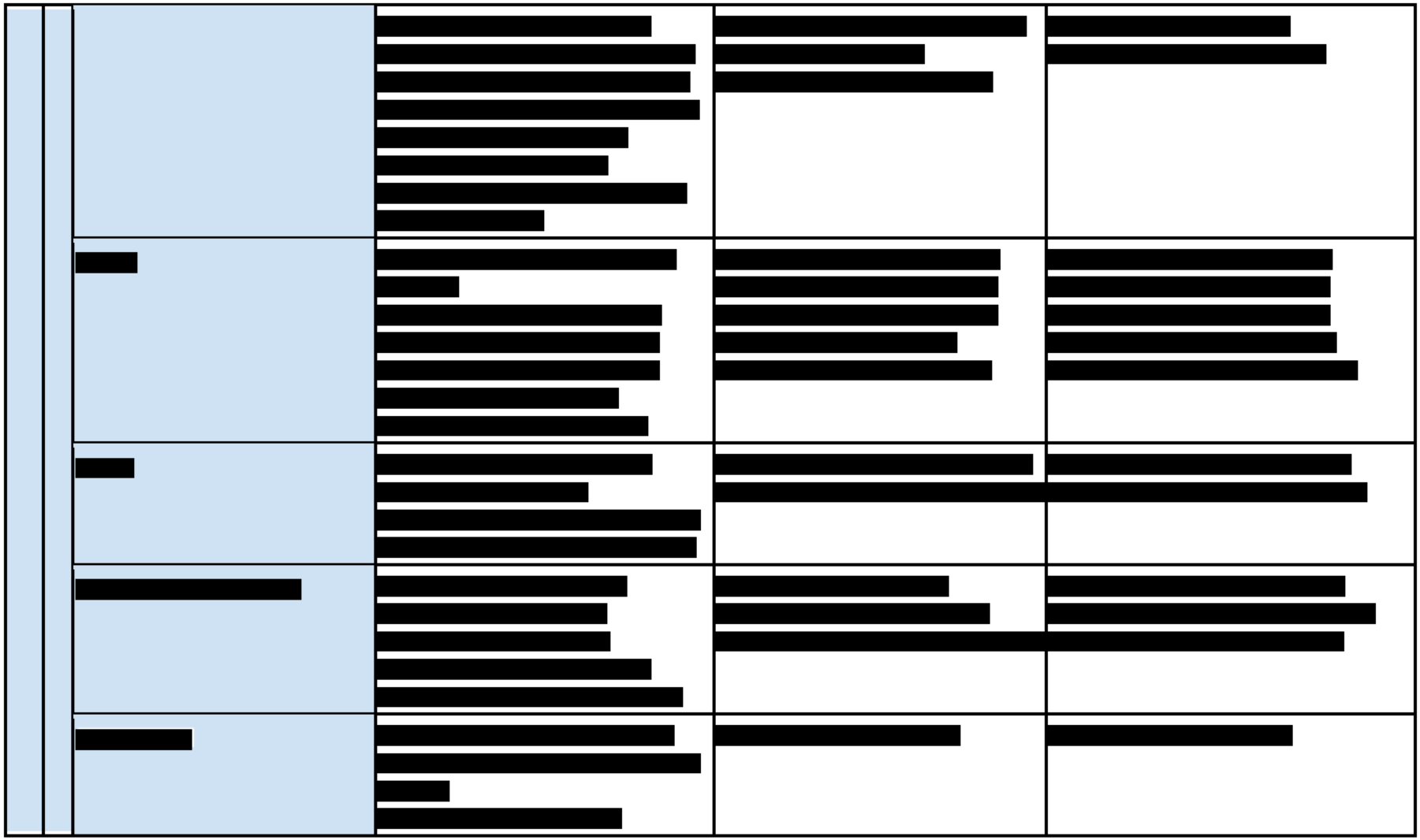
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			
[redacted]			
[redacted]			
[redacted]			

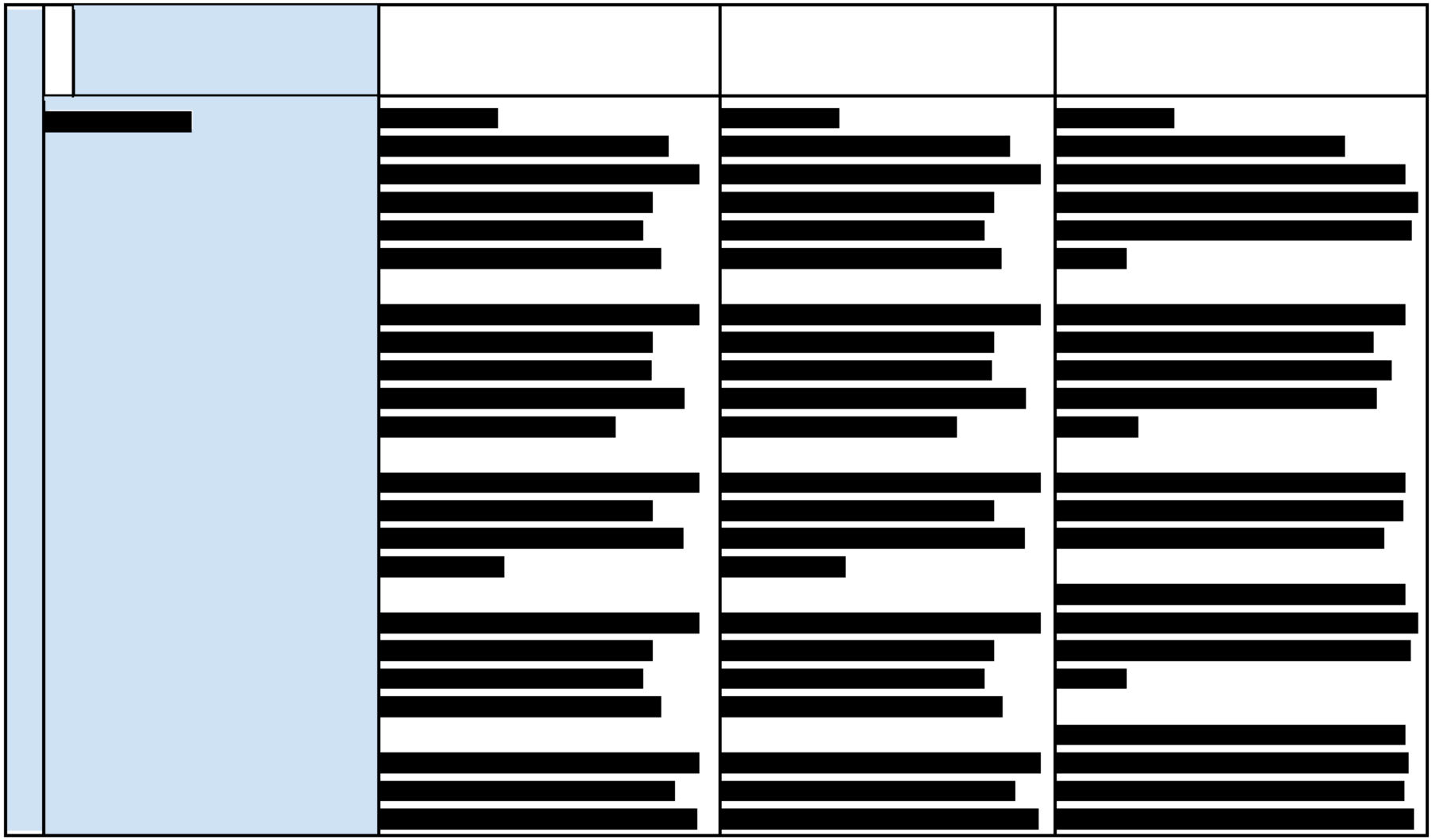
[redacted]

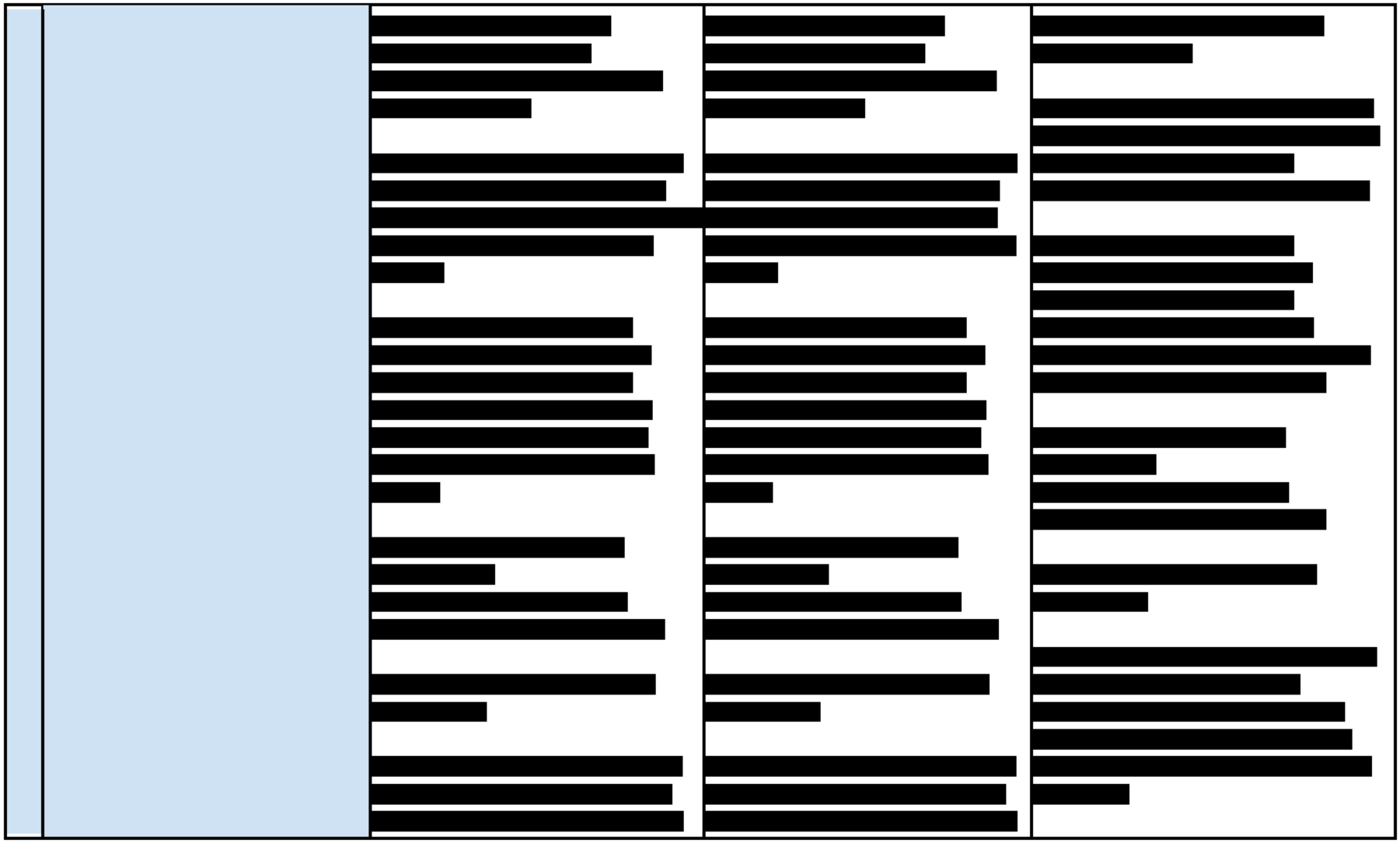
[redacted]			
[redacted]			
[redacted]			
[redacted]			

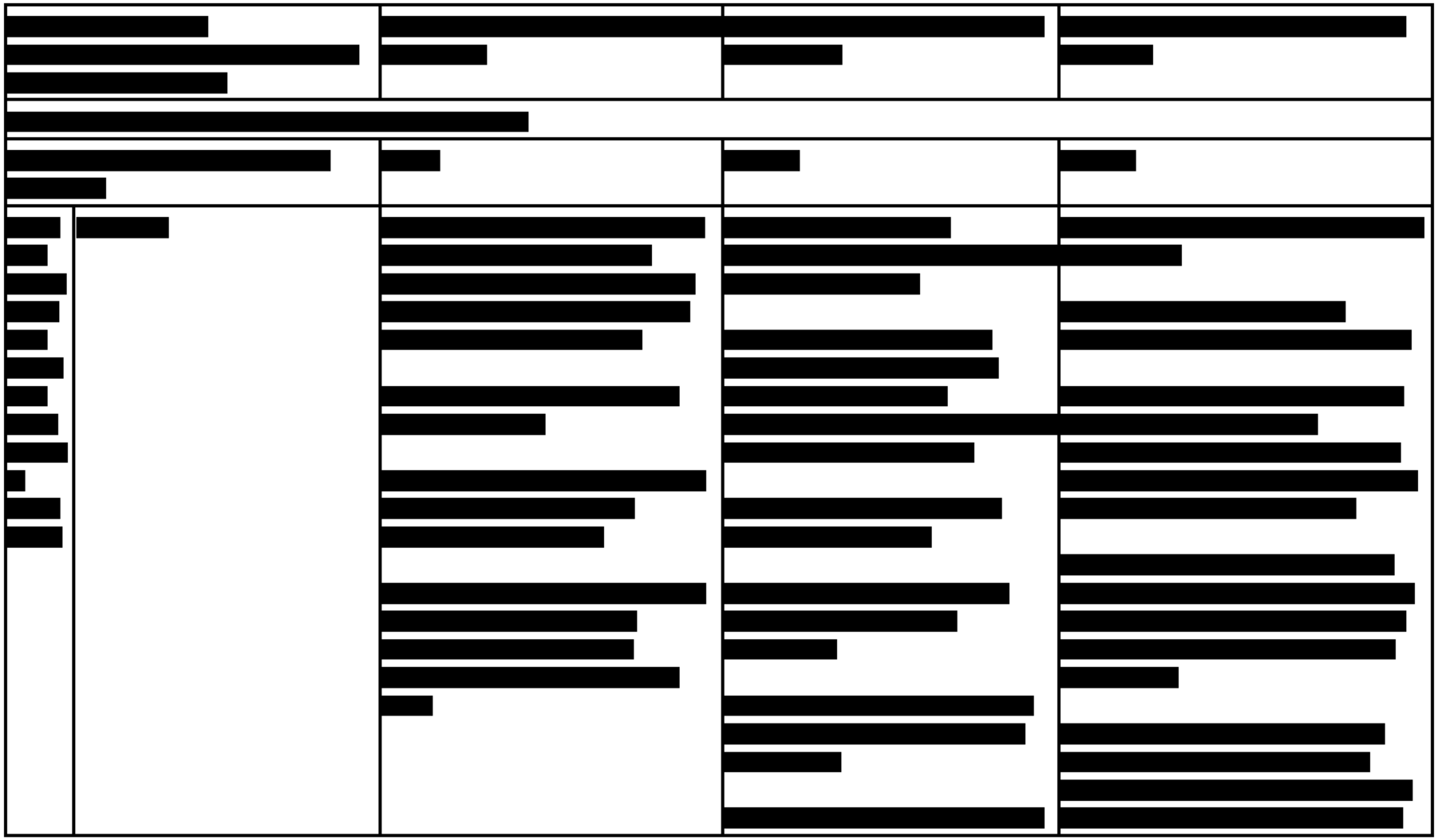
9.5. ANÁLISIS DE RIESGOS









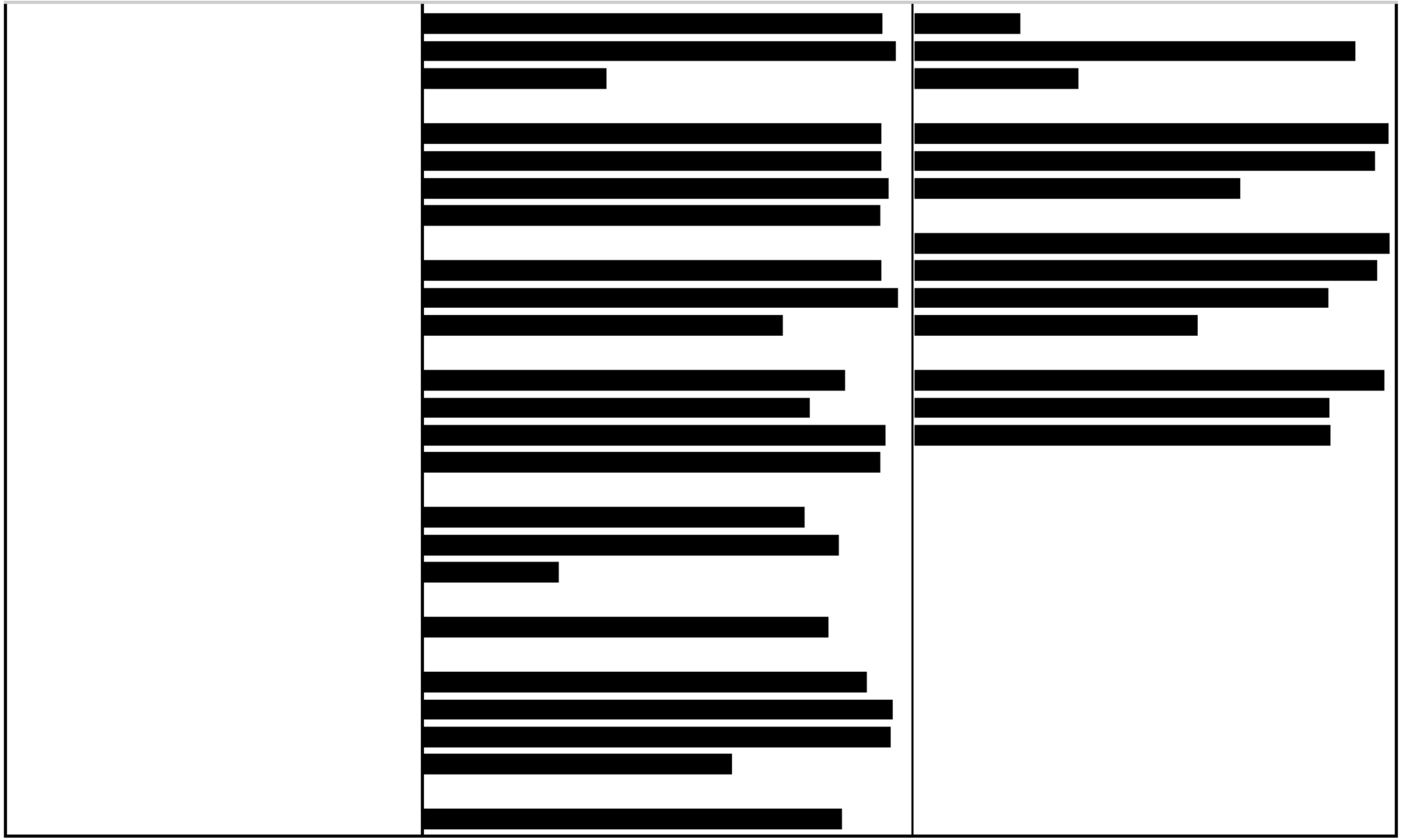


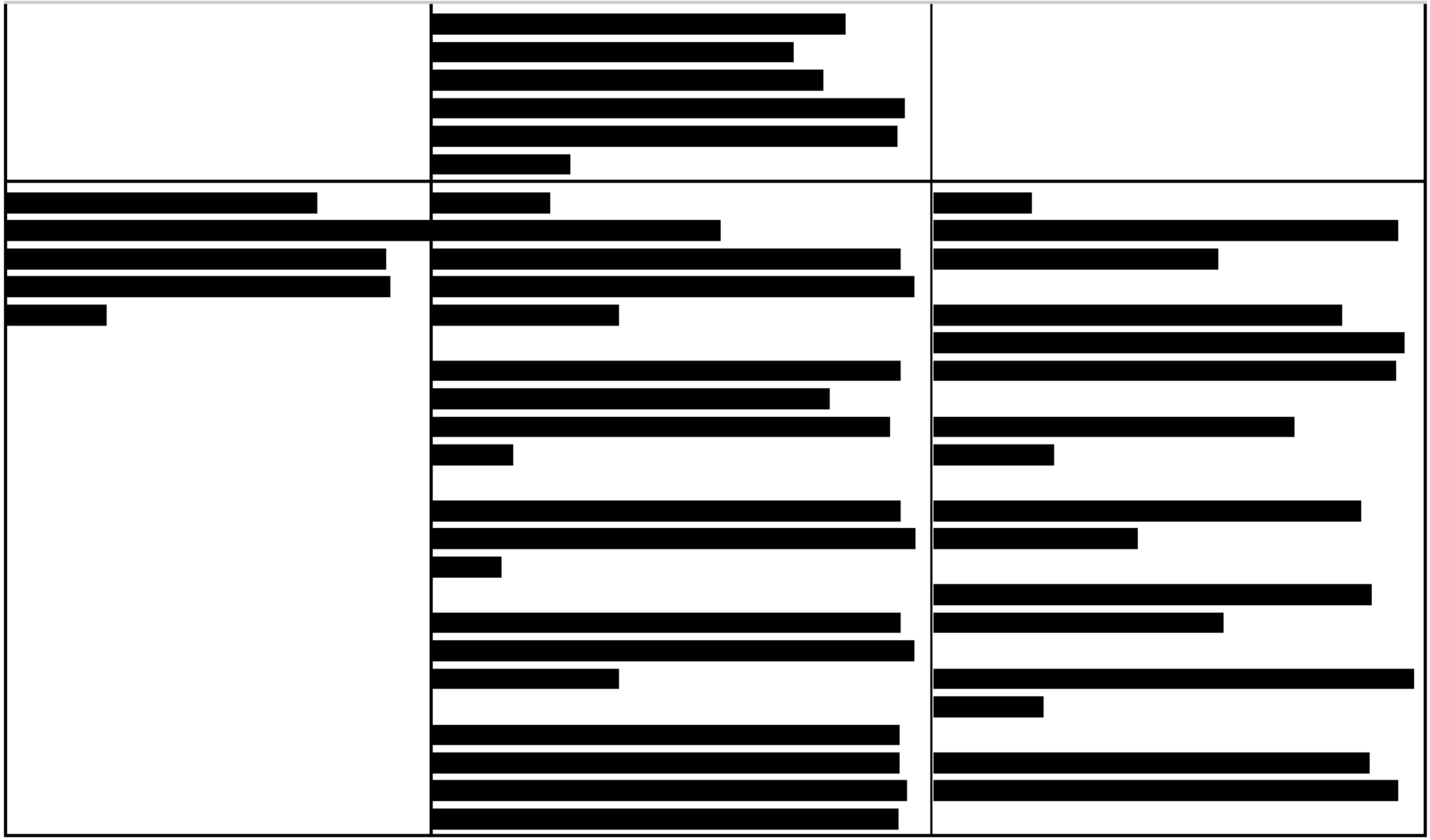
	[redacted]	[redacted]	[redacted]

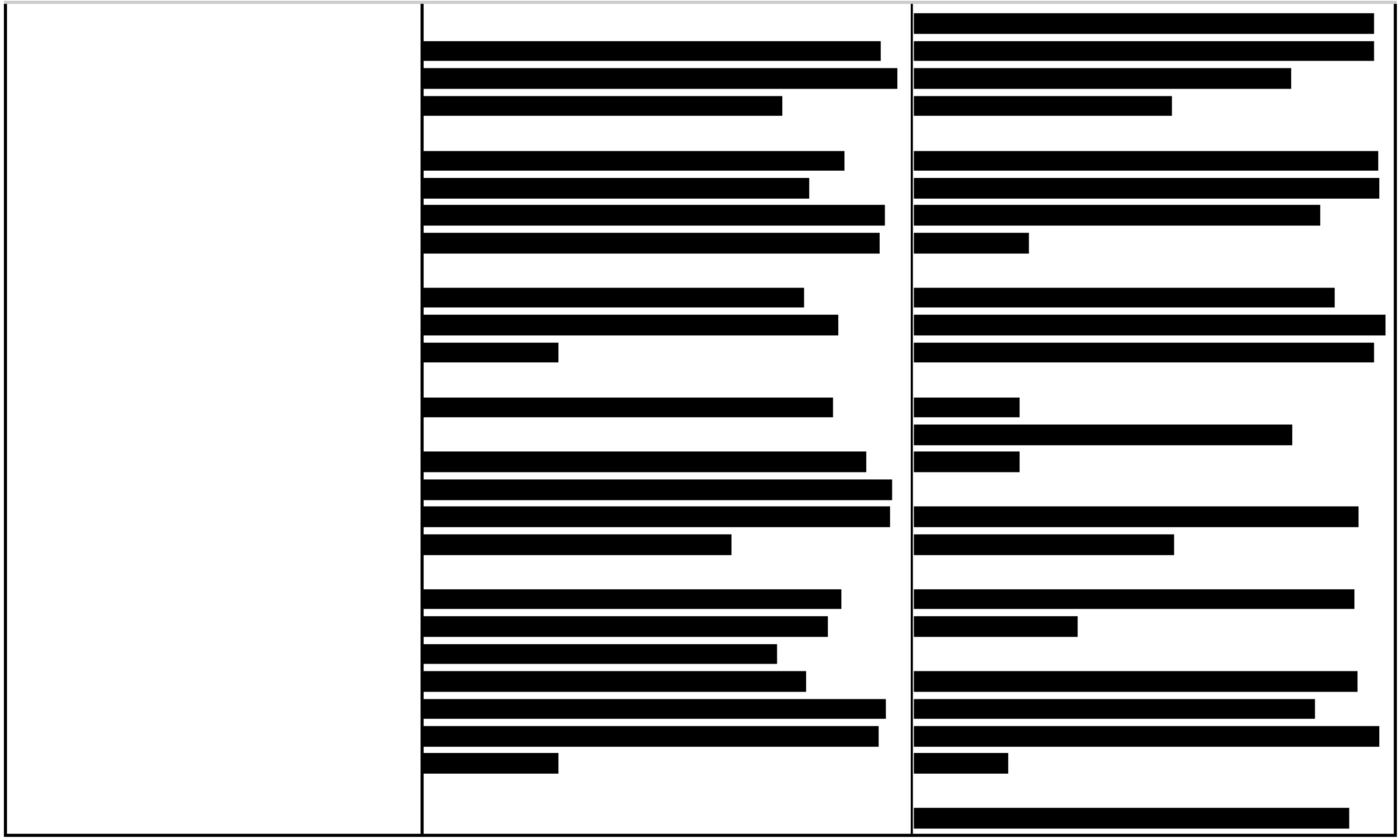
Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI1
Nombre del sistema DTI1	Correo electrónico

ANÁLISIS DE RIESGOS

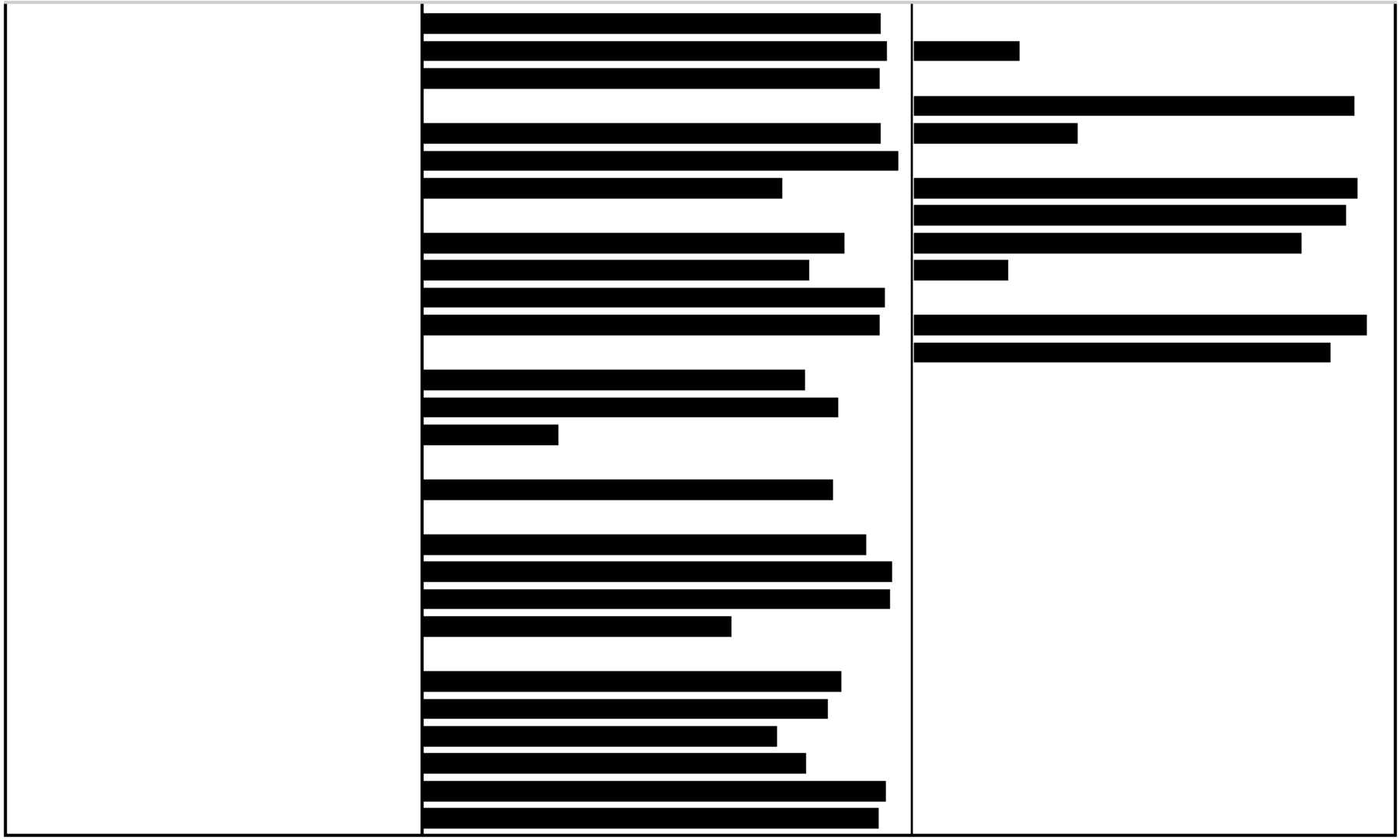
Riesgo	Impacto	Mitigación
[redacted]	[redacted]	[redacted]







		[redacted]
[redacted]	[redacted]	[redacted]

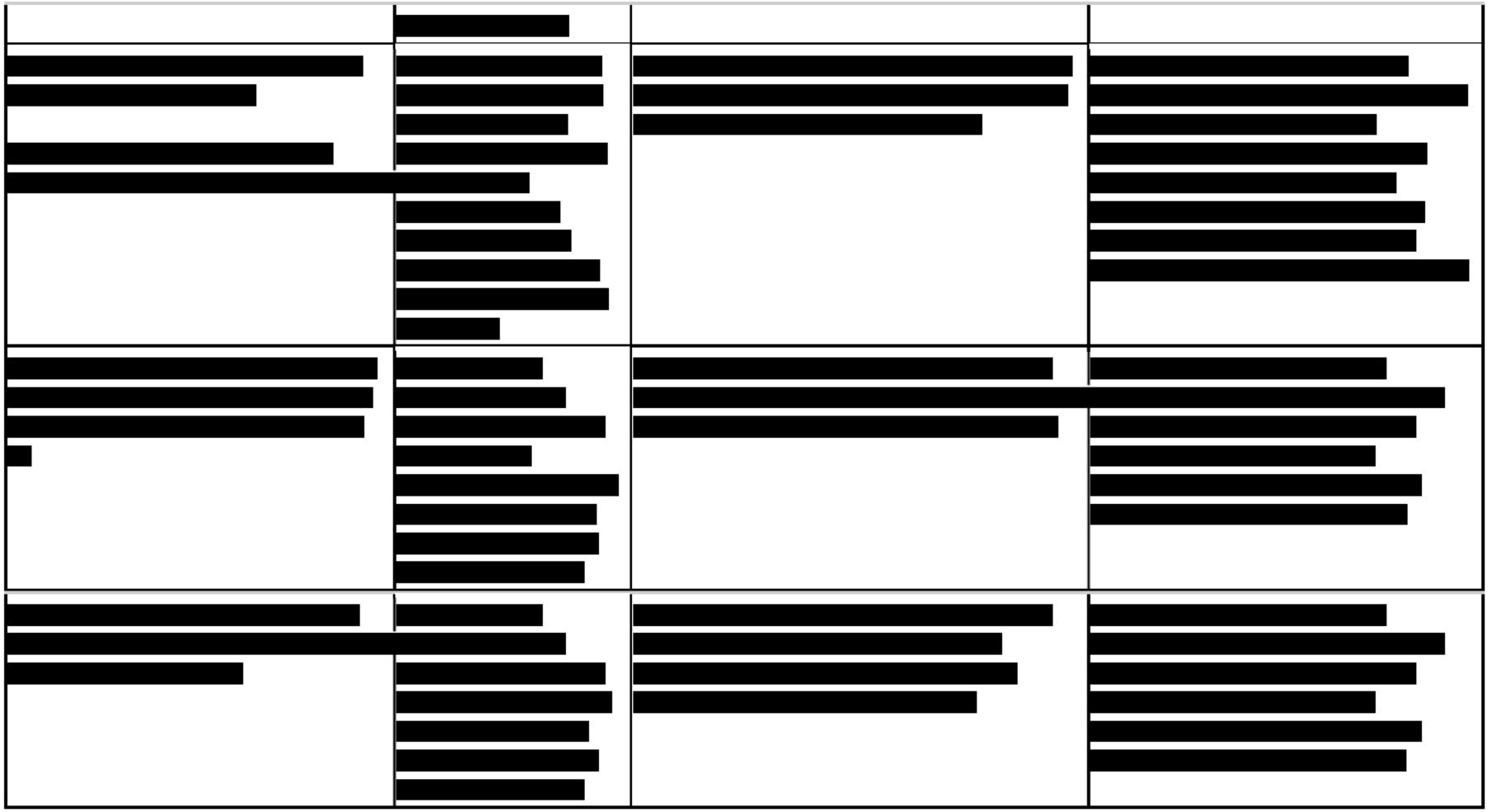


	[redacted]	

9.6. ANÁLISIS DE BRECHA

Desarrollo Tecnológico e Infraestructura, DGRU			
Identificador único	DTI1		
Nombre del sistema DTI1	Correo electrónico		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		

	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		
[redacted]	[redacted]		



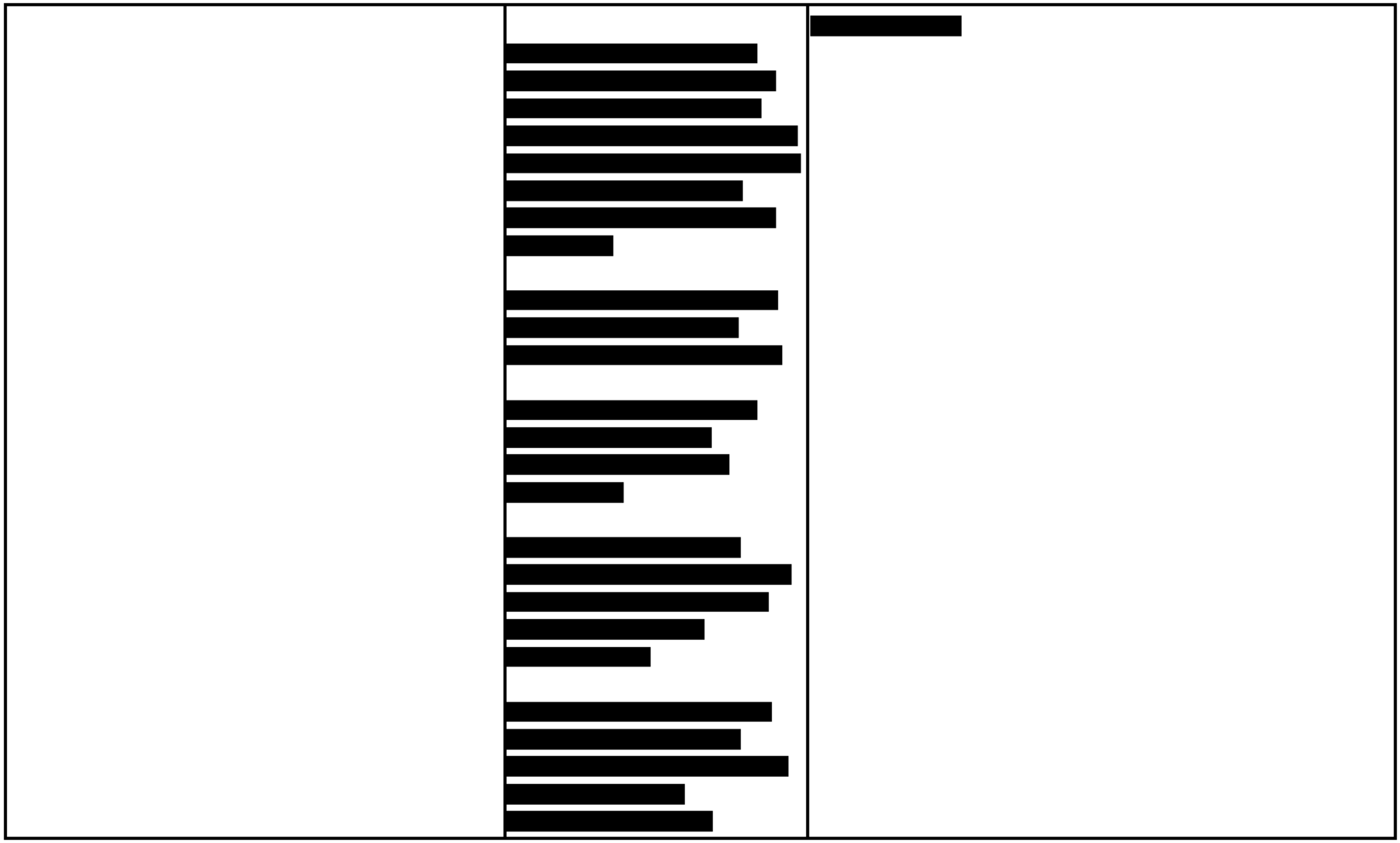
9.7. PLAN DE TRABAJO

Desarrollo Tecnológico e Infraestructura, DGRU				
Identificador único	DTI1			
Nombre del sistema DTI1	Correo electrónico			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]			

9.8. MEDIDAS DE SEGURIDAD

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



	[redacted]	

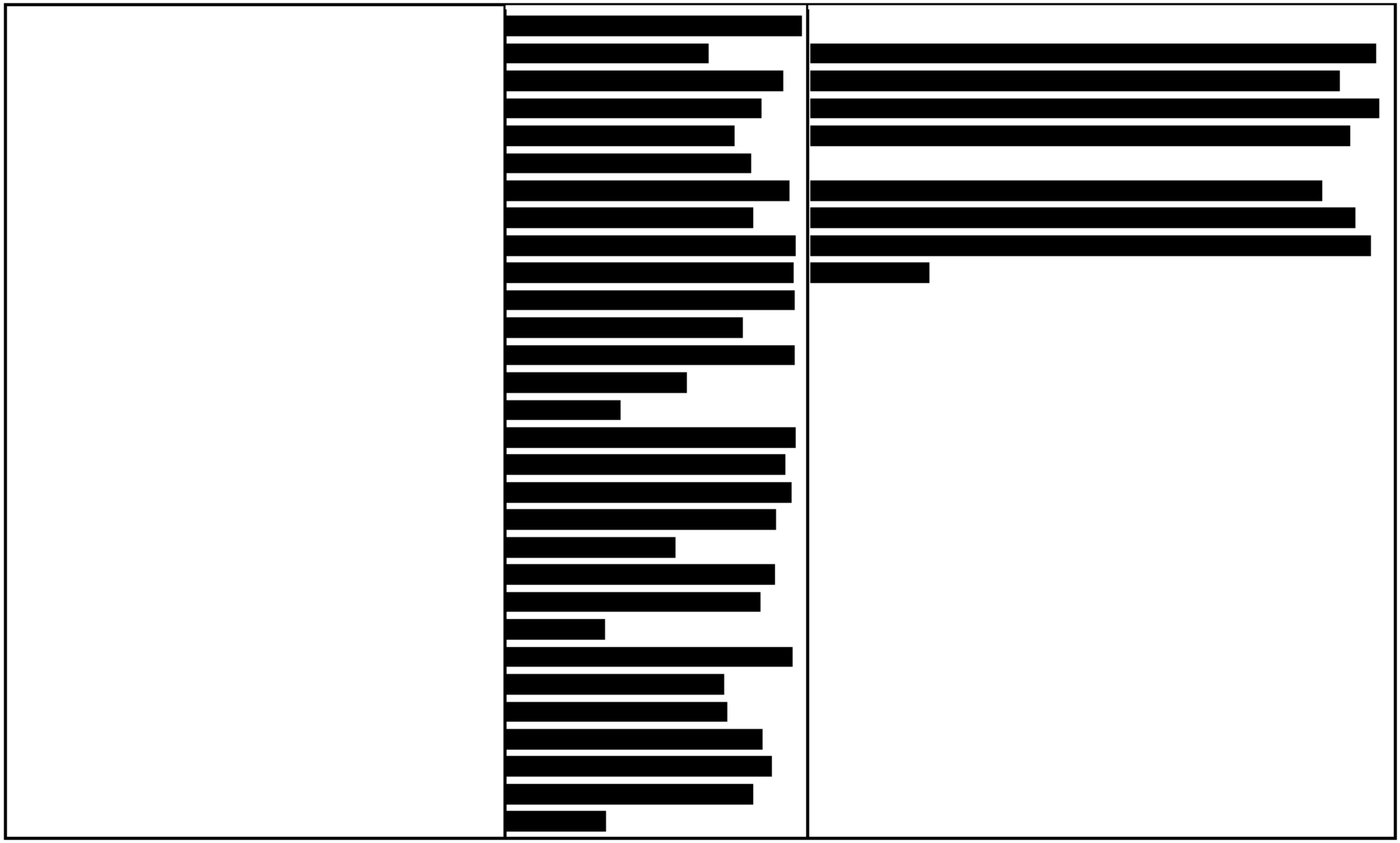
Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI1
Nombre del sistema DTI1	Correo electrónico
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	

[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI1
Nombre del sistema DTI1	Correo electrónico
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA	

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

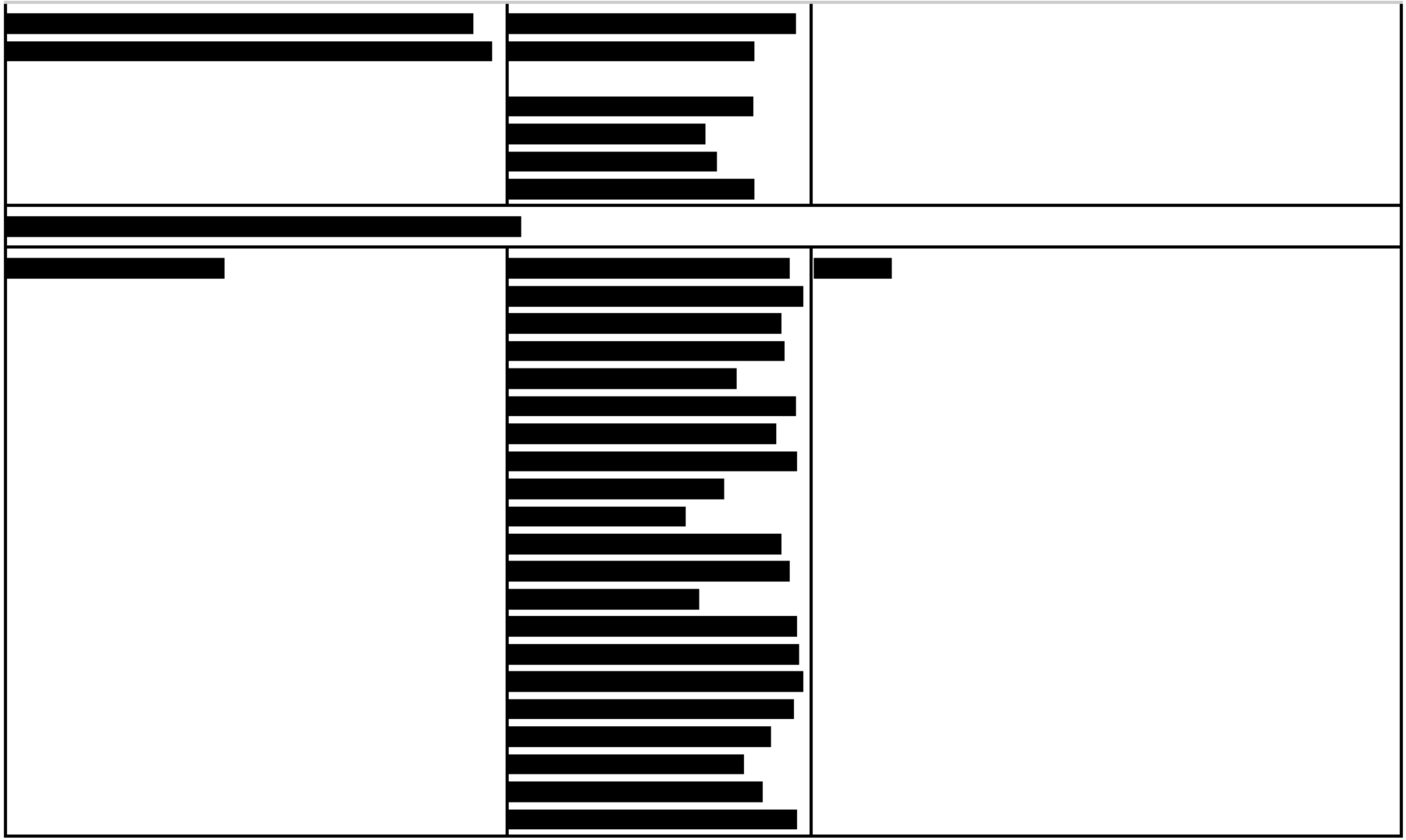
Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
	[redacted]	[redacted]

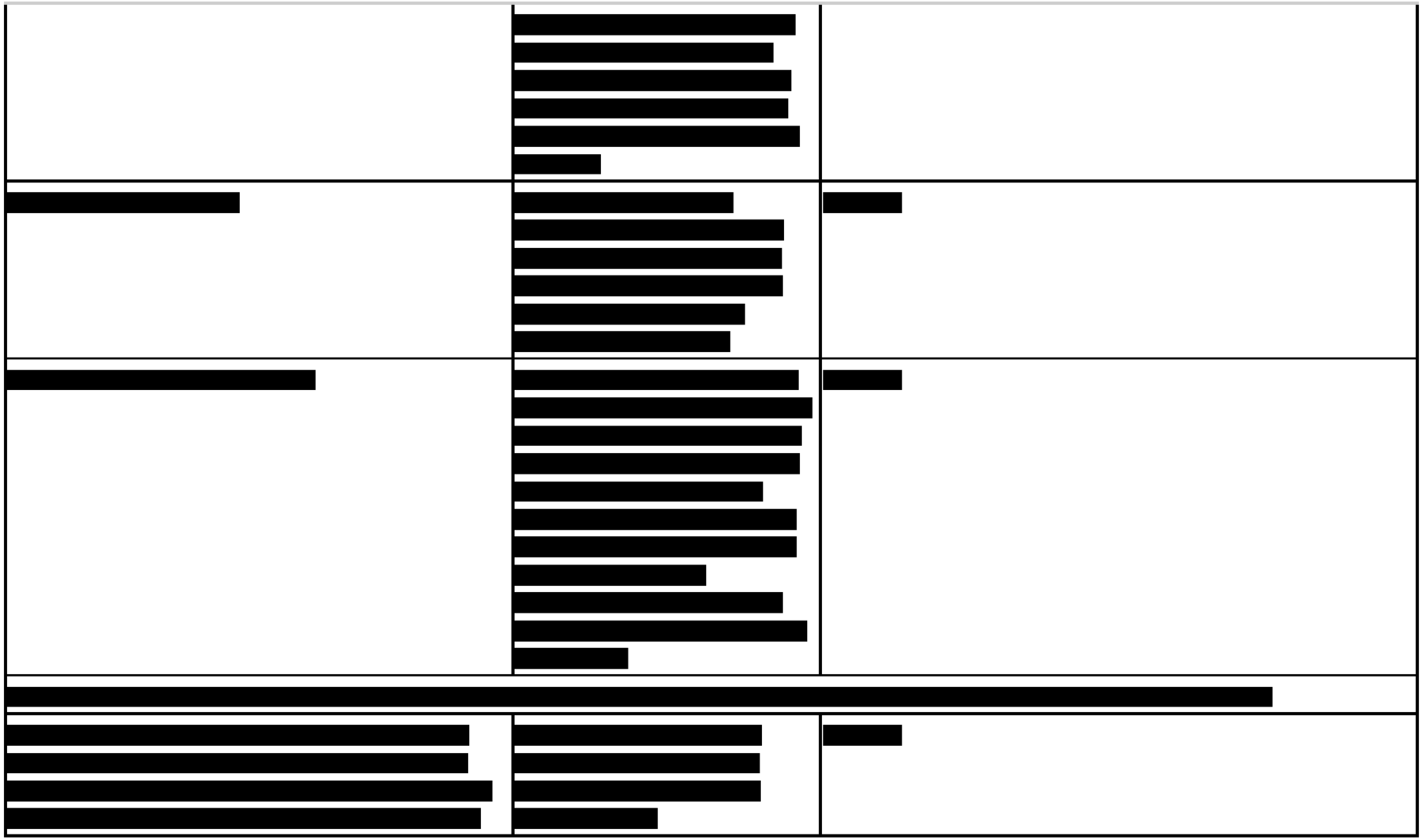
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

[redacted]		
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]



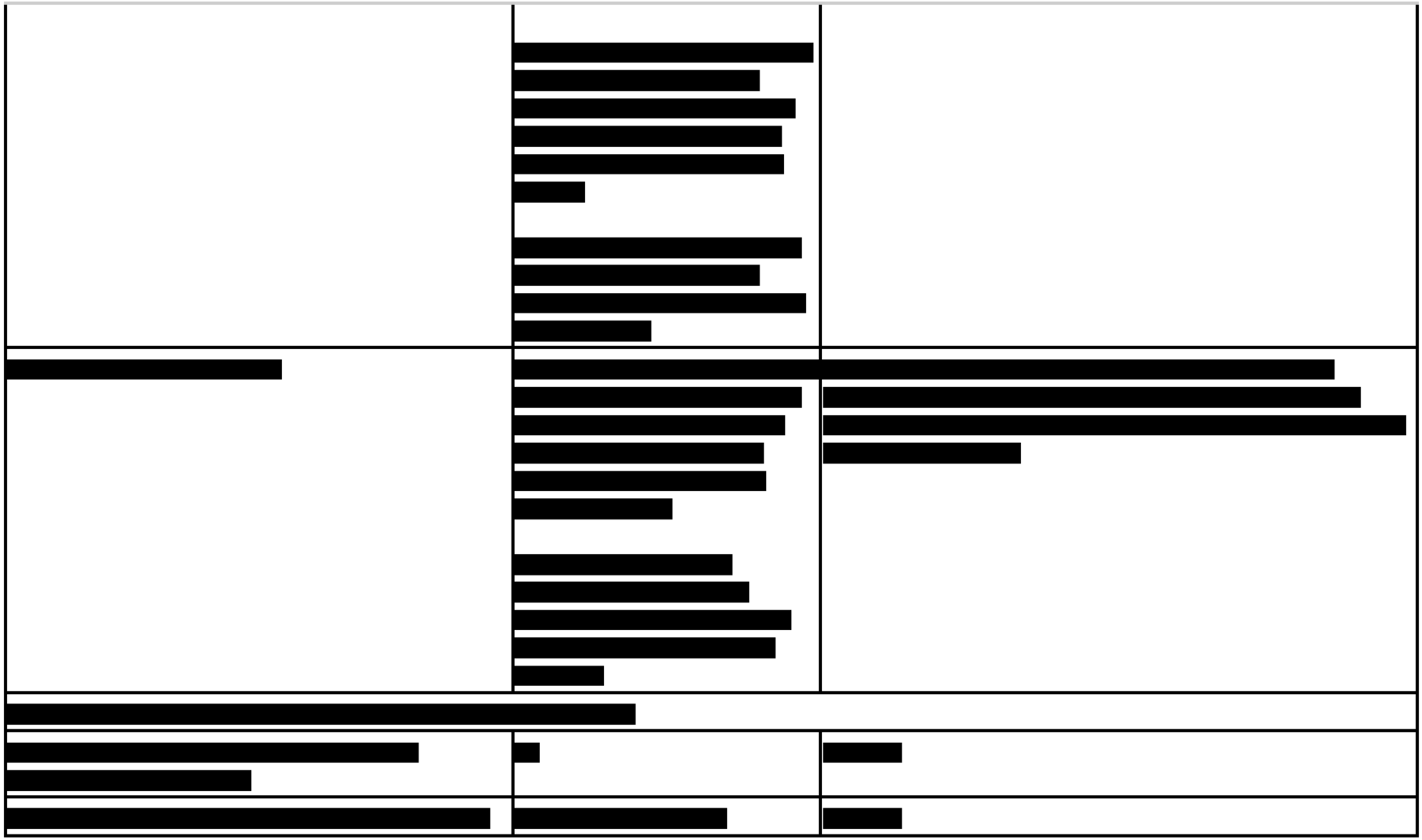


[redacted]		
[redacted]		
[redacted]	[redacted]	[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

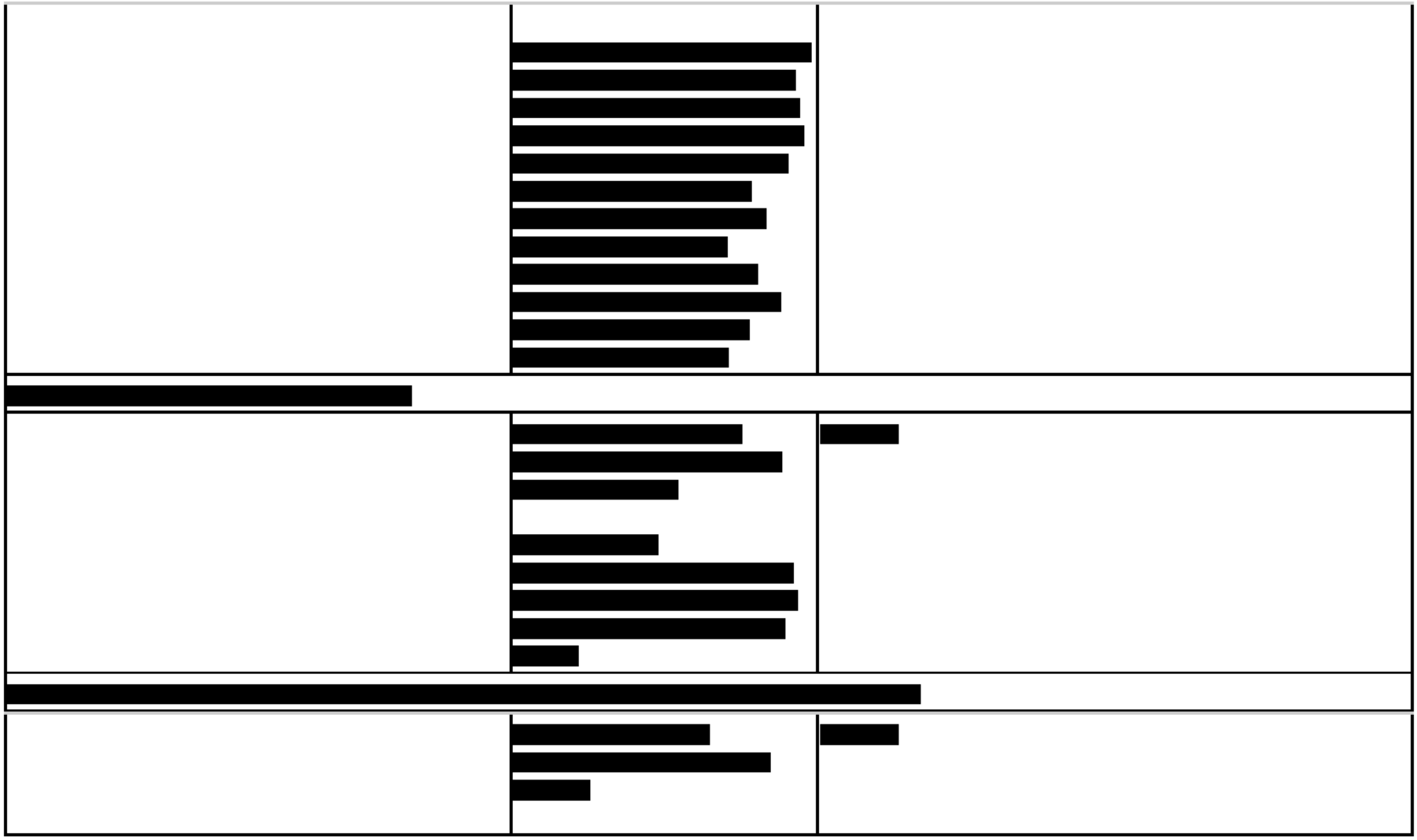
[redacted]		[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.		
[redacted]		
[redacted]	[redacted]	[redacted]



	contraseñas.	

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



	[redacted]	

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
IX. PLAN DE CONTINGENCIA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
	[redacted]	
[redacted]		
	[redacted]	
[redacted]		

[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	

9.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	[redacted]	

Procedimiento para la revisión de las medidas de seguridad

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]

Resultados de la evaluación y pruebas a las medidas de seguridad

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI1	
Nombre del sistema DTI1	Correo electrónico	
Medida de seguridad	**Acciones**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

9.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI1
Nombre del sistema DTI1	Correo electrónico

Actividad	Descripción	Duración	Cobertura	Prioridad
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre protección de datos personales	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	Jornadas variables dependiendo del evento	Responsables de seguridad de datos personales; vigencia y actualización continuas	Alta
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento	Responsables de seguridad de datos personales; vigencia y actualización continuas	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar	Responsables de seguridad de datos personales; vigencia y actualización continuas	Alta

Programa de difusión de la protección a los datos personales

Desarrollo Tecnológico e Infraestructura, DGRU				
Identificador único	DTI1			
Nombre del sistema DTI1	Correo electrónico			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas:	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar	Todo el personal de DGRU. Frecuencia de la actualización una vez al año o	Alta

- Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales. - Procedimientos de borrado seguro de correos electrónicos y de archivos. - Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Uso seguro del correo electrónico y la importancia de cerrar la sesión en los equipos del personal.			antes si se considera necesario	

Anexo 10. DTI2 Cámaras de seguridad

10.1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
Datos personales (sensible o no) contenidos en el sistema:	1. Datos personales en general: Características físicas a partir de imágenes en video.	
¿Cómo se obtienen los datos personales?	Físico ( ) Digital (X)	
¿Para qué se usan?	Se utilizan para procurar la seguridad de las personas y de las instalaciones de la Dirección General de Repositorios Universitarios.	
Los datos se transfieren o se comparten	Si ( ) No (X)	
	¿Con quién se comparten?	¿Para qué?
	Gobierno Federal ( ) Gobierno Estatal ( ) Gobierno Municipal ( ) Personas físicas ( ) Personas morales ( ) Áreas Universitarias ( )	
¿Dónde se alojan?	[redacted]	
¿Cuánto tiempo se da tratamiento?	Permanente en video las 24 hrs. del día por 10 meses consecutivos. Posteriormente el sistema automáticamente borra la información obtenida y reinicia su grabado/registro.	

	Los segmentos copiados del NVR son almacenados al menos por un año en un espacio encriptado de la DGRU, posteriormente son borrados de manera segura.
Responsable	
Nombre:	Tila María Pérez Ortiz
Cargo:	Directora General
Funciones:	Autorizar el tratamiento de los datos personales solicitados.
Obligaciones:	Recibir el oficio y comunicar la solicitud sólo al personal autorizado; autorizar la entrega del segmento de video requerido. Supervisar el proceso sin comprometer la confidencialidad de los datos personales.
Responsable	
Nombre:	Omar Alejandro Solís Garza
Cargo:	Coordinador de Desarrollo Tecnológico e Infraestructura
Funciones:	Supervisión de la operación efectuada mediante procedimientos automatizados aplicados a los datos personales, relacionada con el registro, almacenamiento, acceso y manejo de datos personales.
Obligaciones:	Supervisión de monitoreo y atención de alarmas bajo demanda. Supervisar todo el proceso, sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Dirección General
Co-Responsable	
Nombre:	Roberto Rico Chávez
Cargo:	Jefe de Departamento de Infraestructura, Centro de Datos y Servicios
Funciones:	Operación efectuada mediante procedimientos automatizados aplicados a los datos personales, relacionada con el registro, almacenamiento, acceso y manejo de datos personales.
Obligaciones:	Monitoreo y atención de alarmas bajo demanda. Remitir al Coordinador de Desarrollo

	Tecnológico e Infraestructura segmentos de videos con la información solicitada. Realizar todo el proceso, sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Encargados	
Nombre:	Rogelio Delgado Román
Cargo:	No aplica
Funciones:	Operación efectuada mediante procedimientos automatizados aplicados a los datos personales, relacionada con el registro, almacenamiento, acceso y manejo de datos personales.
Obligaciones:	Monitoreo y atención de alarmas bajo demanda. Remitir al Coordinador de Desarrollo Tecnológico e Infraestructura segmentos de videos con la información solicitada. Realizar todo el proceso, sin comprometer la confidencialidad de los datos personales.
Rinde cuentas a:	Coordinador de Desarrollo Tecnológico e Infraestructura y Dirección General
Usuarios	
Nombre:	No aplica
Cargo:	No aplica
Funciones:	No aplica
Obligaciones:	No aplica

10.2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI2
Nombre del sistema DTI2	Cámaras de seguridad

Tipo de soporte:	[redacted]
Descripción:	[redacted]
Características del lugar donde se resguardan los soportes:	[redacted]

10.3. DESARROLLO DEL PERFIL DE LOS ACTIVOS DE INFORMACIÓN

PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO		
Activo crítico	**Razón de selección**	**Descripción**
¿Cuál es el activo crítico de información?	*¿Por qué es importante el activo de información para la organización?*	*¿Cuál es la descripción condensada del activo de información?*
Grabaciones de video	Porque permiten tener evidencia de lo que sucede en las instalaciones de la Dirección General de Repositorios Universitarios, como apoyo en las medidas de seguridad de las personas e instalaciones.	Archivos de videograbaciones de las instalaciones de la DGRU que pueden contener imágenes de personas.
Dueño		
¿A quién pertenece el activo de información?		
Directora General		
Requisitos de seguridad		
¿Cuáles son los requisitos de seguridad para el activo de información?		
(X) Confidencialidad	Solo personal autorizado puede acceder a este activo de información de la siguiente manera:	Las imágenes en video se considerarán confidenciales toda vez que pueden incluir datos personales y únicamente personal autorizado podrá acceder a ellos.
(X) Integridad	Solo personal autorizado puede modificar a este activo de información de la siguiente manera:	La información únicamente podrá ser modificada por personal autorizado de la DGRU.
(X) Disponibilidad	Este activo debe estar disponible para que el personal realice sus labores de la siguiente manera:	La información contenida en los archivos de videograbaciones debe estar disponible cuando sea necesaria su consulta.

	Este activo debe estar disponible 24 horas, 7 días/semana, 52 semanas/año.	La información contenida en los archivos de videograbaciones debe estar disponible las 24 hrs, para cubrir casos de emergencia o vulneración de la seguridad de las personas, instalaciones o equipos.
( ) Otro		

Requisitos de seguridad más importante			
¿Cuál es el requisito de seguridad más importante para este activo?			
(X) Confidencialidad	**( ) Integridad**	**( ) Disponibilidad**	**( ) Otro**

MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (TÉCNICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**

[redacted]	[redacted]
[redacted]	[redacted]
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (FÍSICO)	
INTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
EXTERNO	
DESCRIPCIÓN DE CONTENEDOR	**DUEÑO(S)**
[redacted]	
MAPAS DE AMBIENTES DE RIESGO DEL ACTIVO DE INFORMACIÓN (HUMANO)	
INTERNO	
NOMBRE O FUNCIÓN / RESPONSABILIDAD	**ÁREA**
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
EXTERNO	

NOMBRE O FUNCIÓN / RESPONSABILIDAD	DUEÑO(S)
[redacted]	

10.4. RIESGO DE ACTIVO DE INFORMACIÓN

RIESGO DE ACTIVO DE INFORMACIÓN	
Activo de información	Cámaras de seguridad
Área de preocupación	[redacted]

CONTENEDORES TÉCNICOS

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]

[redacted]

[redacted]					
[redacted]					
[redacted]					
[redacted]					

CONTENEDORES FÍSICOS

No aplica

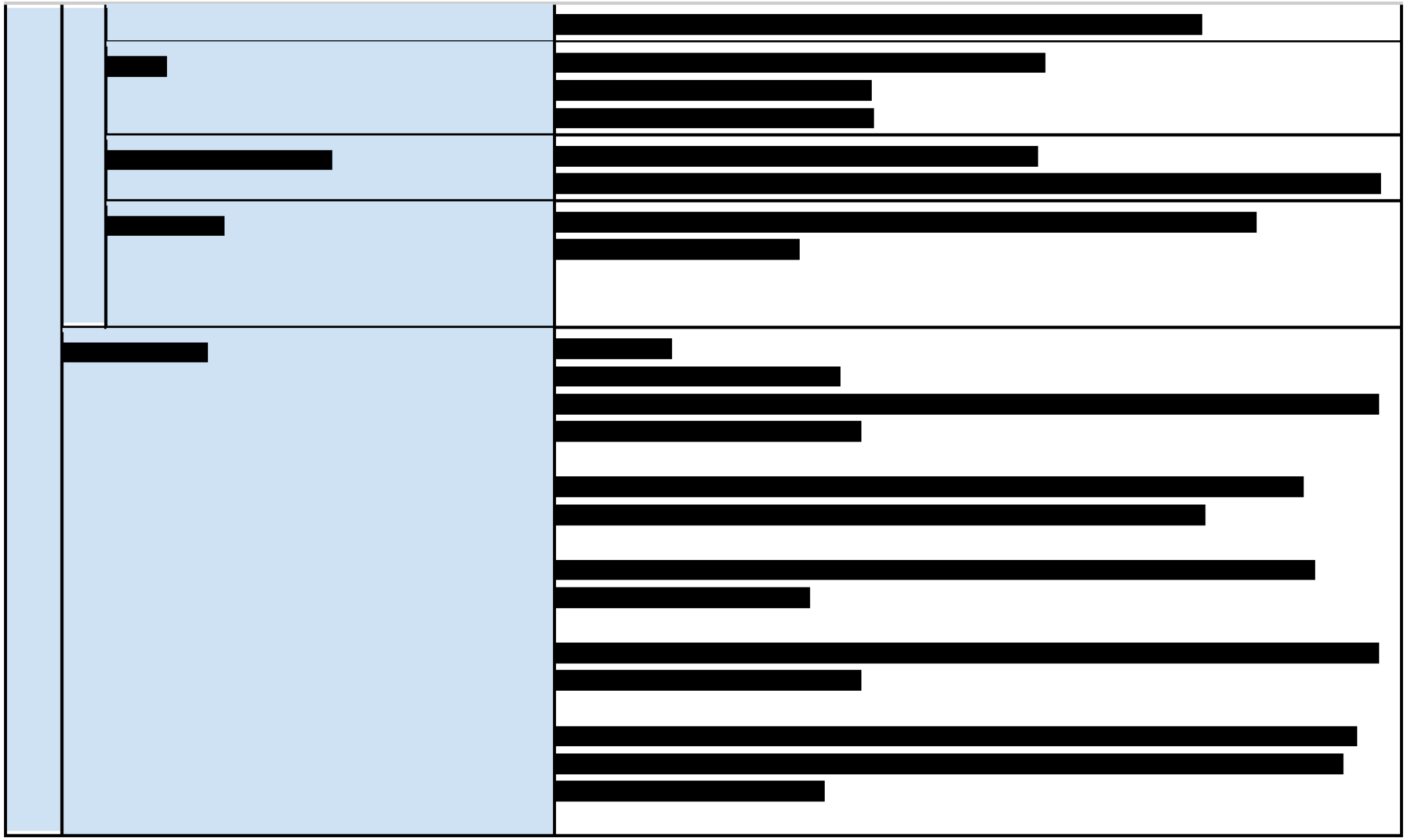
RECURSOS HUMANOS

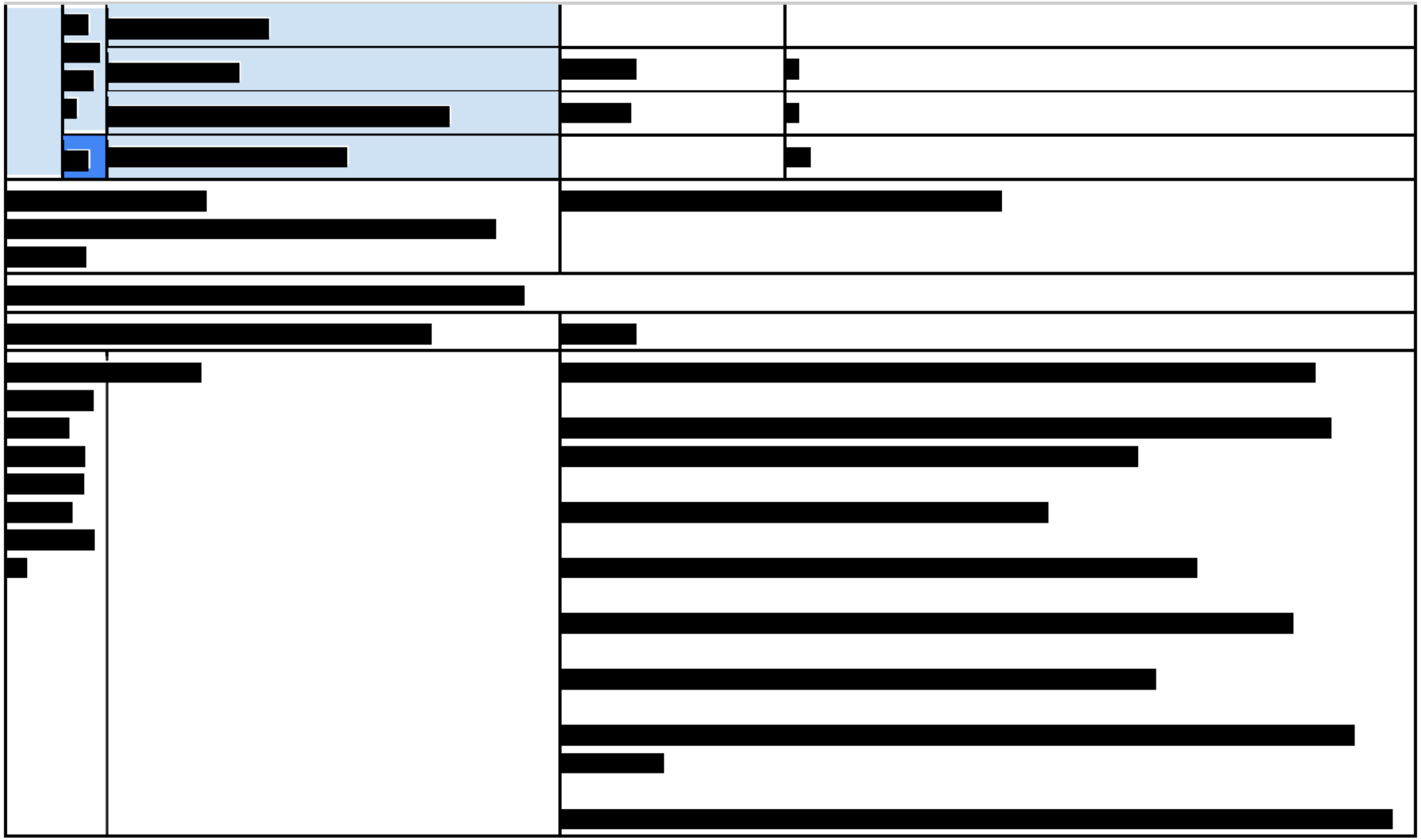
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			

[redacted]

10.5. ANÁLISIS DE RIESGOS

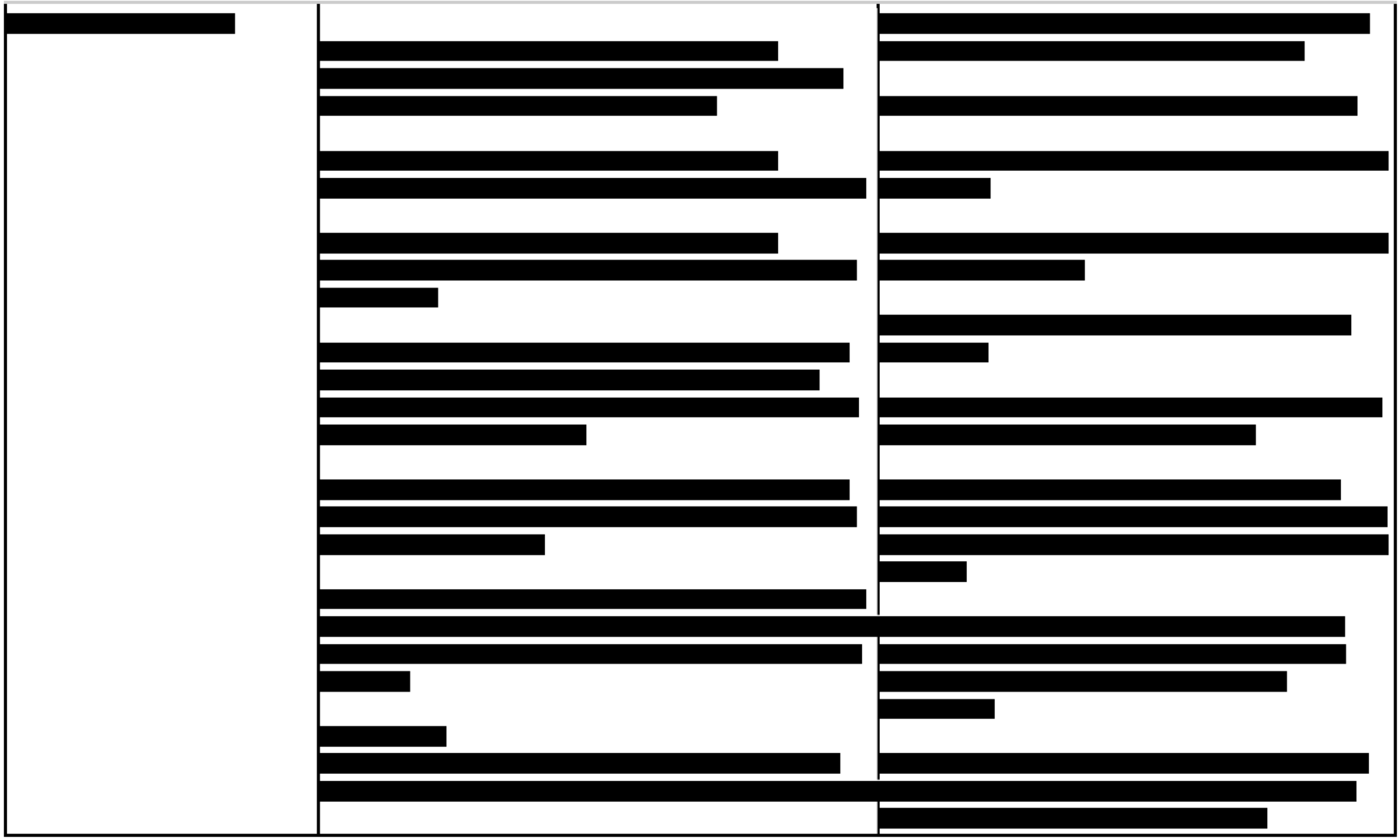
[redacted]

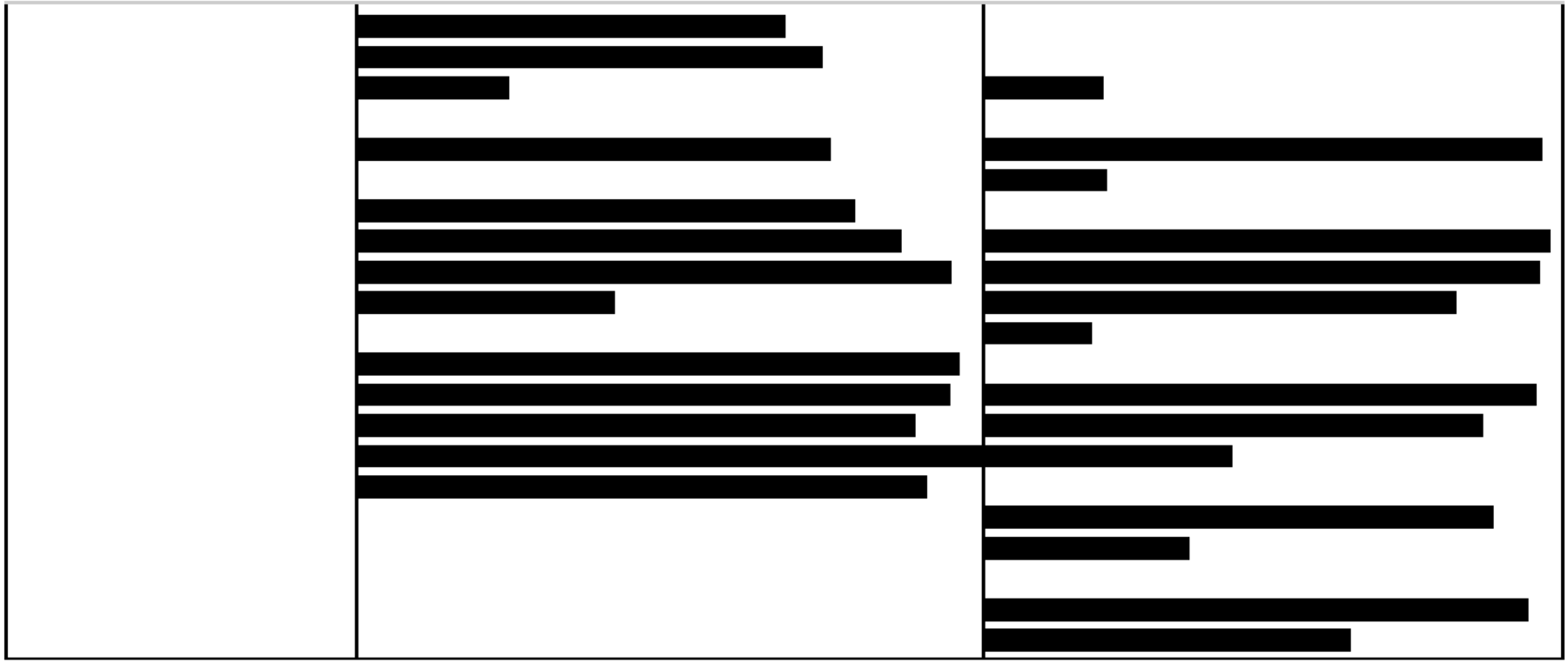




[redacted]	[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
ANÁLISIS DE RIESGOS		
Riesgo	**Impacto**	**Mitigación**
[redacted]	[redacted]	[redacted]

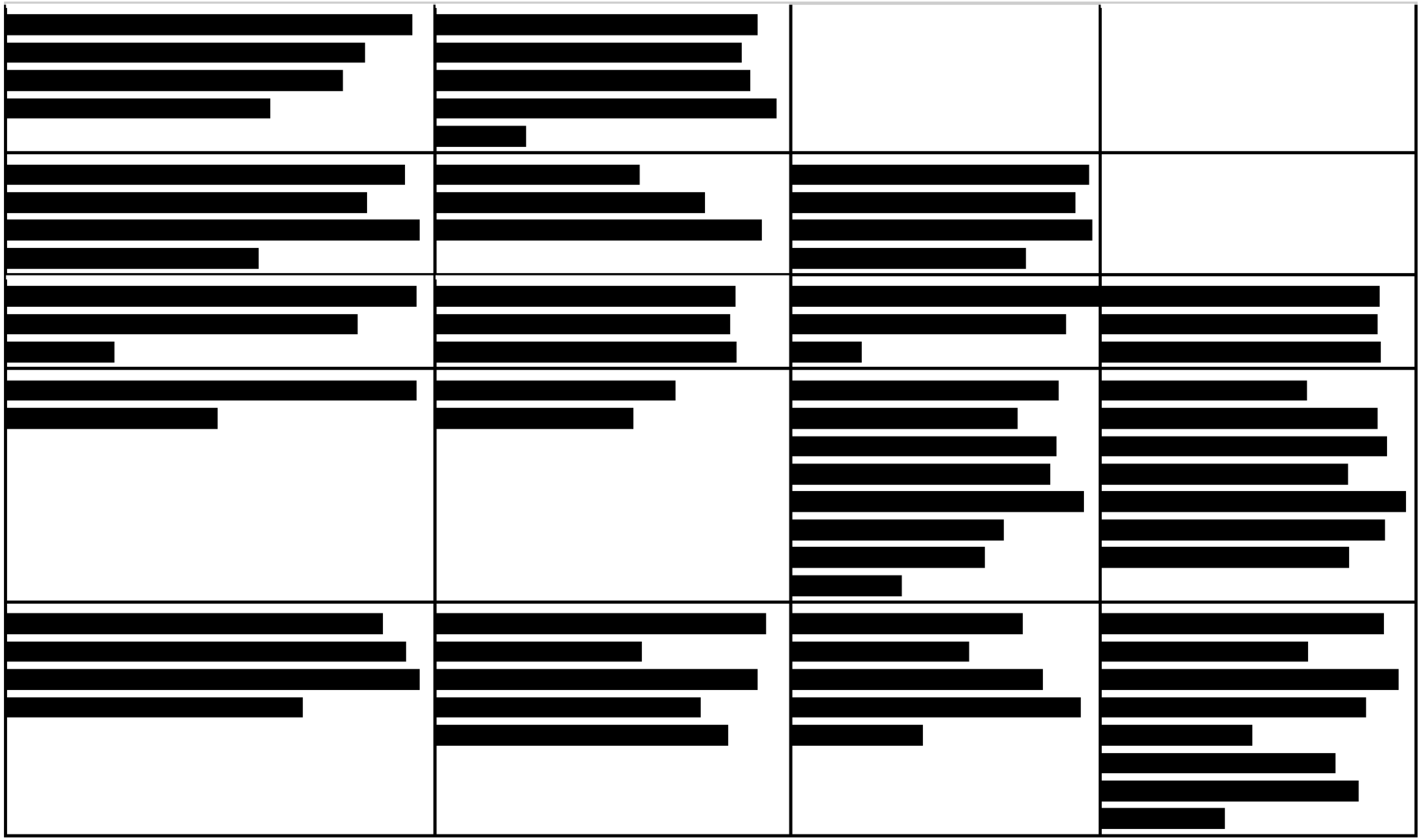


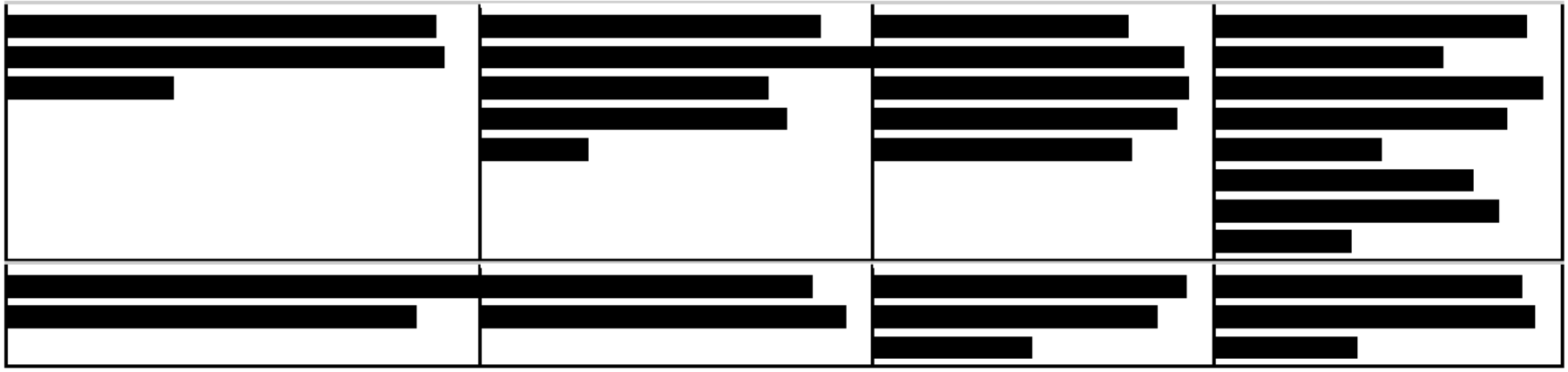


10.6. ANÁLISIS DE BRECHA

Desarrollo Tecnológico e Infraestructura, DGRU			
Identificador único	DTI2		
Nombre del sistema DTI2	Cámaras de seguridad		
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**	**¿Qué se necesita?**

[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		





10.7. PLAN DE TRABAJO

Desarrollo Tecnológico e Infraestructura, DGRU				
Identificador único	DTI2			
Nombre del sistema DTI2	Cámaras de seguridad			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]		[redacted]	
[redacted]	[redacted]		[redacted]	

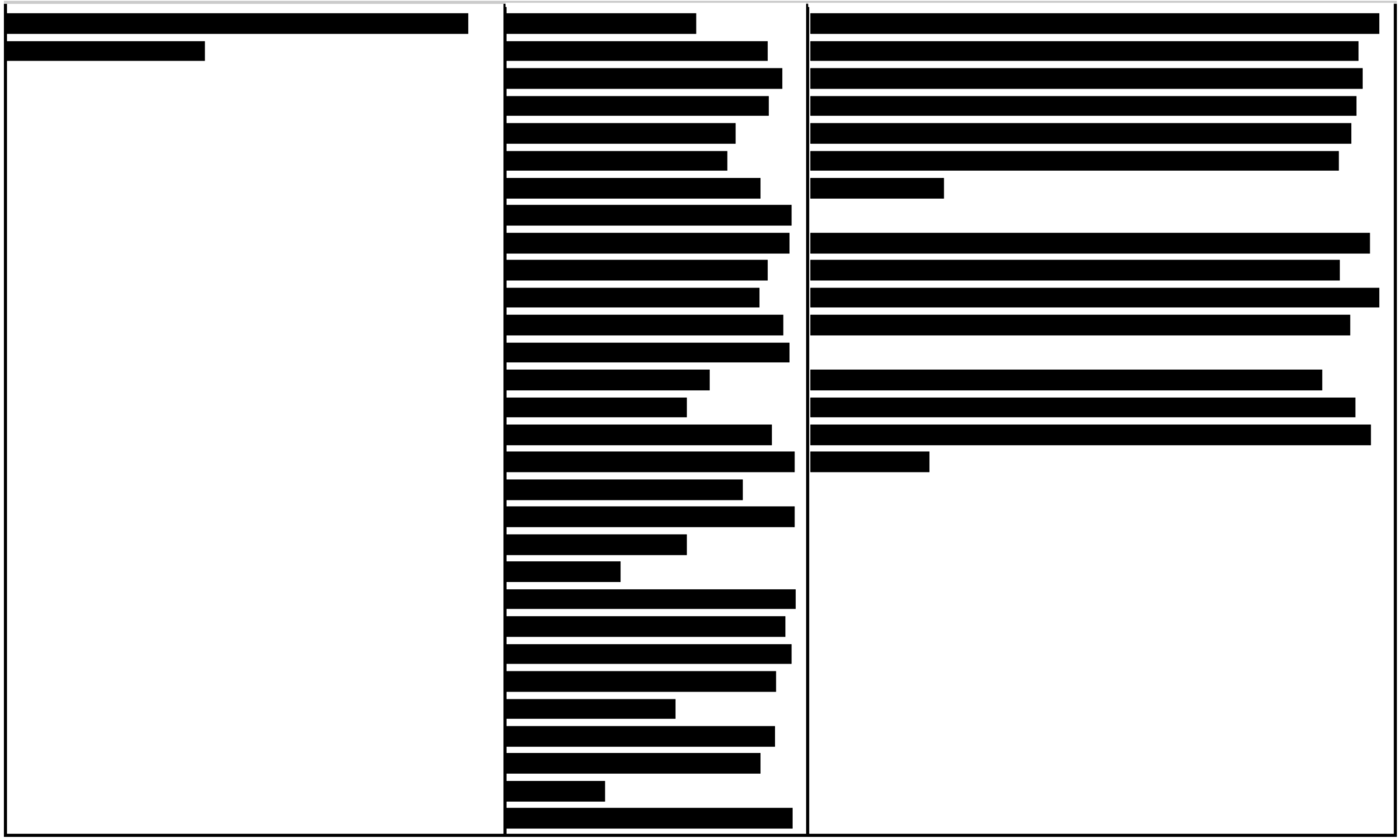
10.8. MEDIDAS DE SEGURIDAD

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
I. TRANSFERENCIAS DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI2
Nombre del sistema DTI2	Cámaras de seguridad
II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS	
[redacted]	

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	



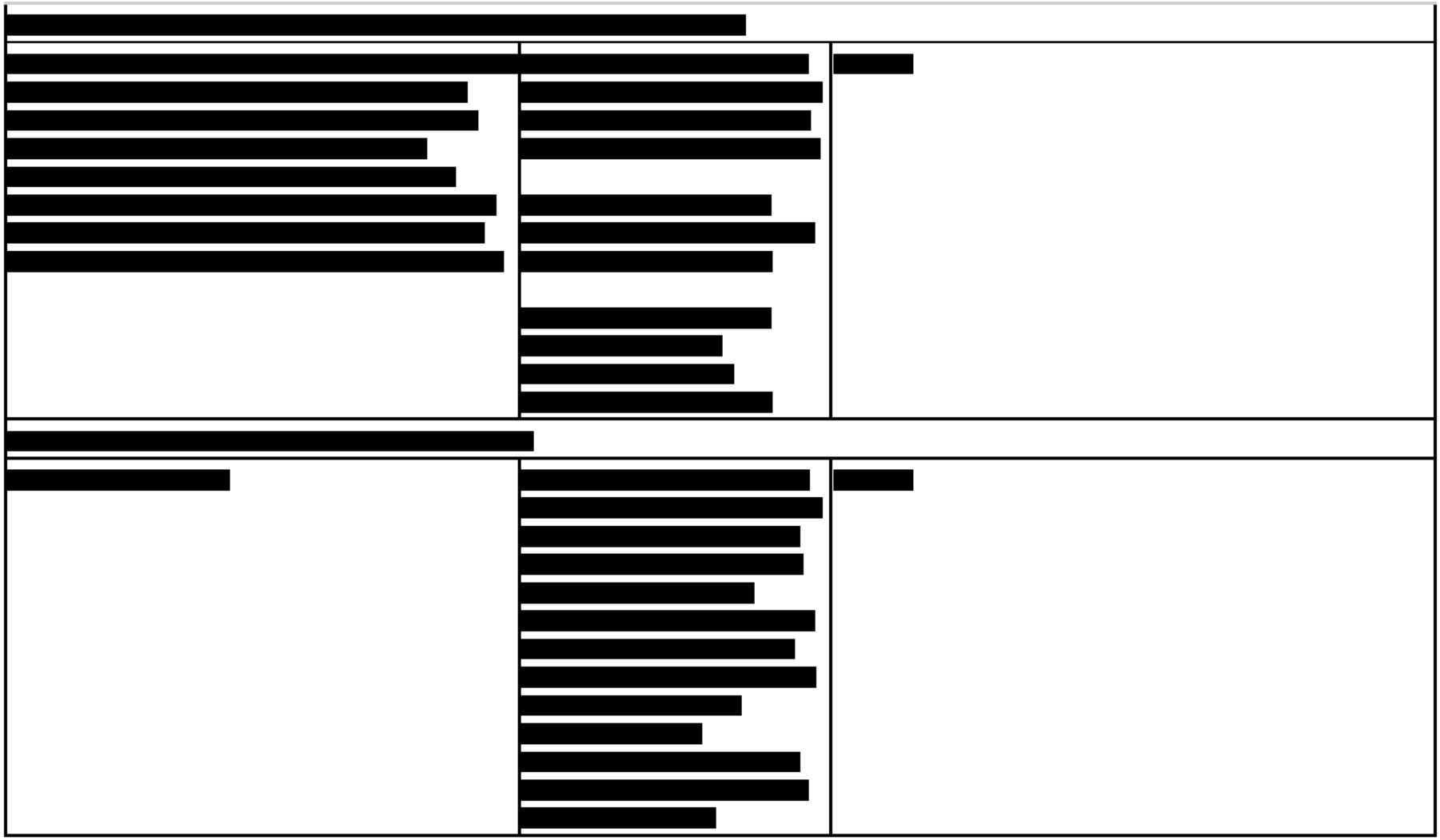
[redacted]		

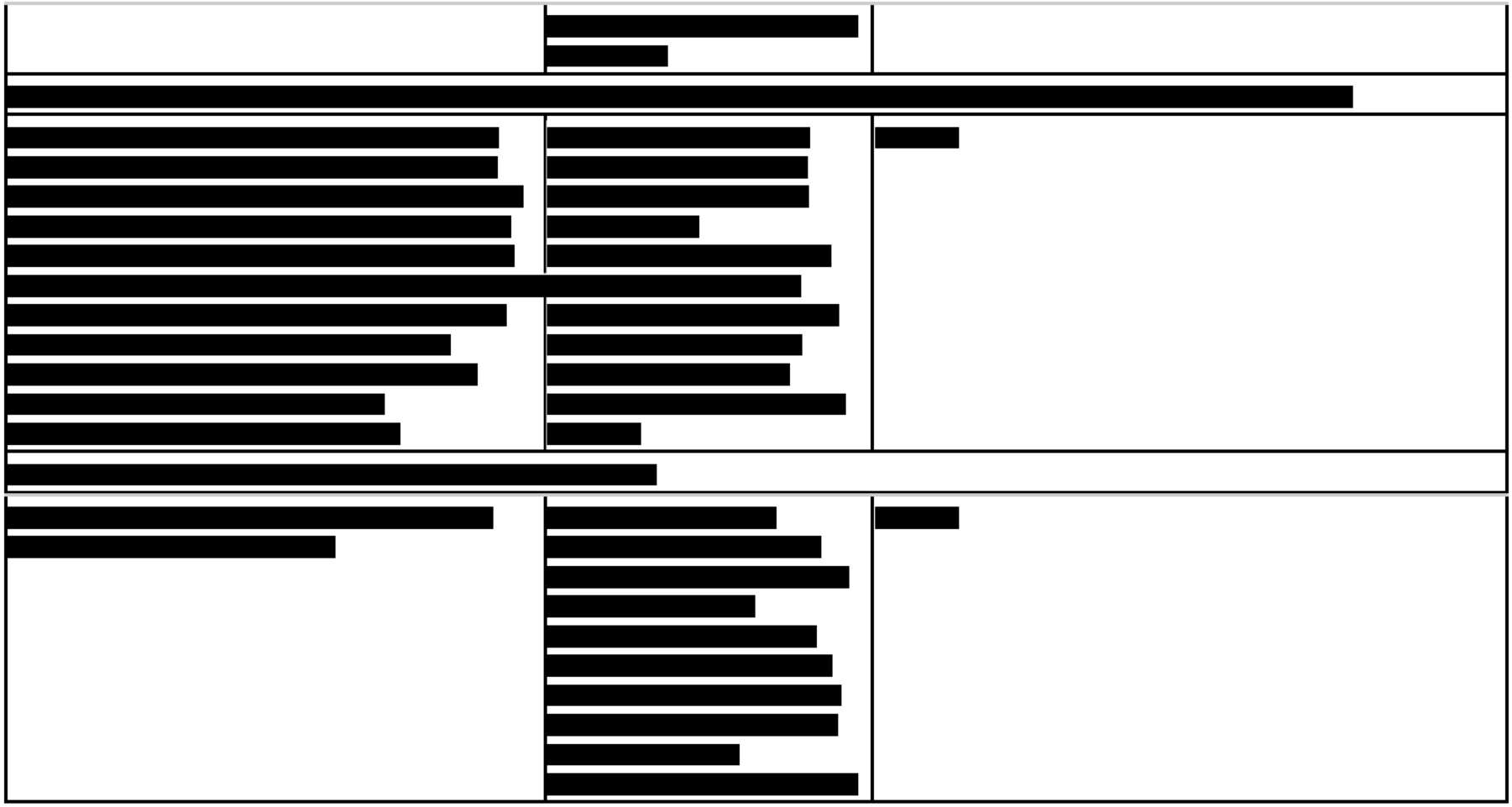
Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI2
Nombre del sistema DTI2	Cámaras de seguridad

IV. REGISTRO DE INCIDENTES		
	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]
[redacted]		
	[redacted]	[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
V. ACCESO A LAS INSTALACIONES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**





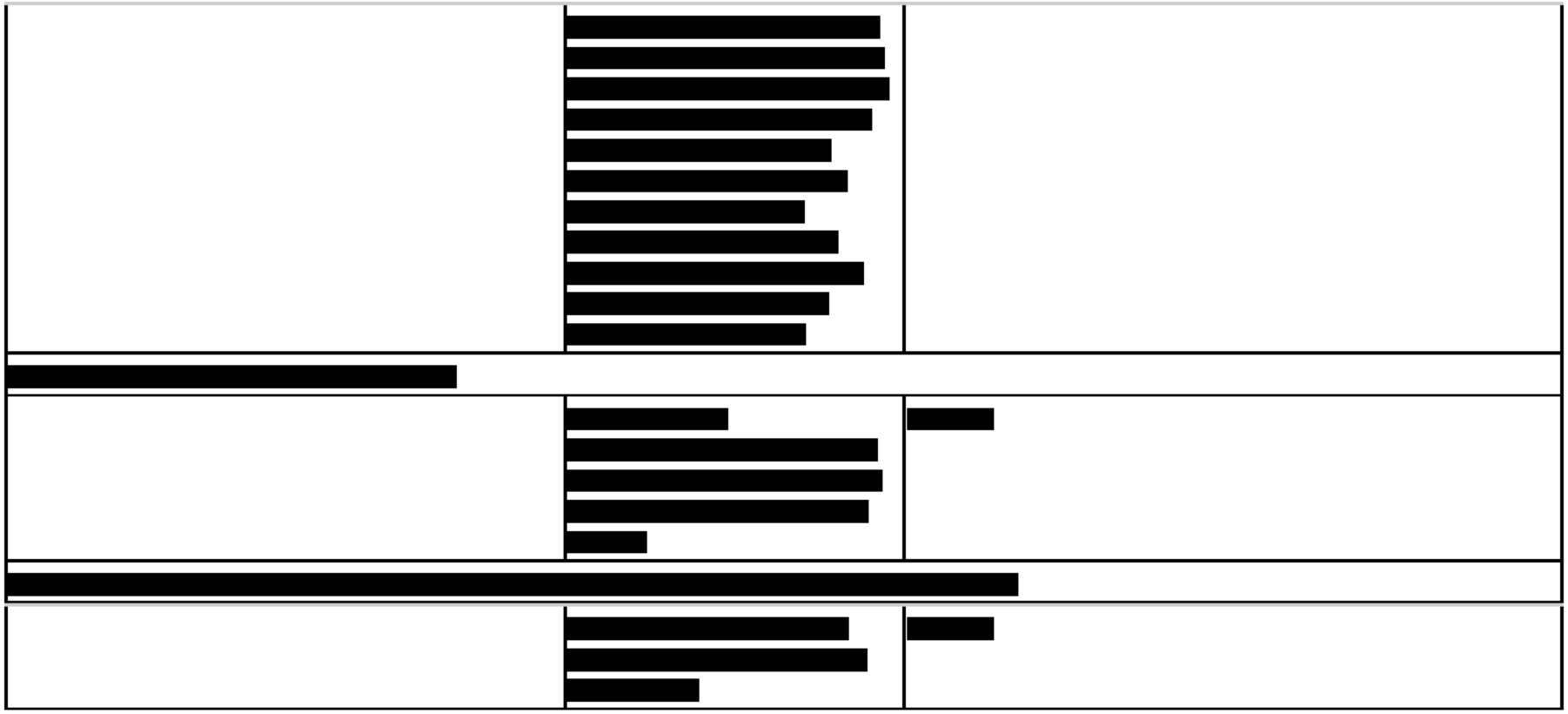
Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]	[redacted]	[redacted]

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
VII. PERFILES DE USUARIO Y CONTRASEÑAS		
	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		
[redacted]	[redacted]	[redacted]

[redacted]		

Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI2
Nombre del sistema DTI2	Cámaras de seguridad
VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS	

	MEDIDAS APLICADAS	**MEDIDAS POR APLICAR**
[redacted]		



Desarrollo Tecnológico e Infraestructura, DGRU	
Identificador único	DTI2
Nombre del sistema DTI2	Cámaras de seguridad
IX. PLAN DE CONTINGENCIA	

	MEDIDAS APLICADAS	MEDIDAS POR APLICAR
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

10.9. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Herramientas y recursos para monitoreo de la protección de datos personales

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
Recurso	**Descripción**	**Control**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]

Procedimiento para la revisión de las medidas de seguridad

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
Medida de seguridad	**Procedimiento**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	[redacted]	

Resultados de la evaluación y pruebas a las medidas de seguridad

Desarrollo Tecnológico e Infraestructura, DGRU		
Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Acciones para la corrección y actualización de las medidas de seguridad

Desarrollo Tecnológico e Infraestructura, DGRU

Identificador único	DTI2	
Nombre del sistema DTI2	Cámaras de seguridad	
Medida de seguridad	Acciones	Responsable
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

10.10. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

Programa de capacitación a los responsables de seguridad de datos personales

Dirección General, DGRU				
Identificador único	DTI2			
Nombre del sistema IJ1	Cámaras de Seguridad			
Actividad	Descripción	Duración	Cobertura	Prioridad
Asistir a eventos convocados por la Unidad de Transparencia u otra entidad o dependencia universitaria sobre	Diversas entidades o dependencias universitarias pueden organizar eventos en materia de Protección de Datos Personales que	Jornadas variables dependiendo del	Responsables de seguridad de datos personales; vigencia y	Alta

protección de datos personales.	pueden fortalecer las estrategias de seguridad internas o para el cumplimiento de la normatividad aplicable.	evento.	actualización continuas.	
Dar seguimiento a eventos nacionales, internacionales e institucionales en materia de Protección de Datos Personales.	Asistir o dar seguimiento a eventos para estar al día sobre las tendencias en materia de protección de datos personales a nivel nacional e internacional.	Jornadas variables dependiendo del evento.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Media
Divulgación interna de normatividad e información relevante en términos de Protección de Datos personales.	Monitorear la publicación de normatividad o información relevante en materia de datos personales para revisar dicha documentación y analizar los alcances, implicaciones y posibles acciones requeridas.	Sesiones variables, dependiendo de los temas a tratar.	Responsables de seguridad de datos personales; vigencia y actualización continuas.	Alta

Programa de difusión de la protección a los datos personales

Dirección General, DGRU				
Identificador único	DTI2			
Nombre del sistema IJ1	Cámaras de Seguridad			
Actividad	**Descripción**	**Duración**	**Cobertura**	**Prioridad**
Desarrollar un programa de difusión de la protección a los datos personales y el material de apoyo correspondiente, en el que se aborden los siguientes temas: - Importancia de llevar a cabo buenas prácticas en todo el quehacer cotidiano para dar un adecuado y cuidadoso tratamiento de datos personales.	El programa de difusión se realizará de manera virtual o presencial con sesiones previamente agendadas para revisar el material generado para este fin.	Sesiones variables, dependiendo de los temas a tratar.	Personal de las coordinaciones de Desarrollo Tecnológico e Infraestructura, Sistema de Repositorios Universitarios, Colecciones de Datos e	Alta

- Dar a conocer el nombre de las personas autorizadas para acceder al archivo y divulgarla al menos una vez al año. - Procedimientos de borrado seguro de correos electrónicos y de archivos. - Uso adecuado de sesiones en la plataforma y en los equipos del personal.			Investigación, de Planeación, Gestión y Normatividad y Dirección General. Frecuencia de la actualización una vez al año o antes si se considera necesario.	

Anexo 11. Criterios de medición del riesgo

Los criterios de medición del riesgo son un conjunto de criterios cualitativos con los que se puede evaluar el efecto del riesgo contra la misión y objetivos de la organización [1]. En la DGRU se consideraron los siguientes:

CRITERIOS DE MEDICIÓN DEL RIESGO
Reputación y confianza
Financiera
Productividad
Seguridad y salud
Multas y penas legales

[1] Lugo Rojas Esther (febrero 2020). Análisis de riesgos en seguridad informática. Coordinación de Seguridad de la Información.

Para cada uno de los criterios se proponen áreas de impacto, es decir, se presuponen condiciones de cómo la DGRU se verá afectada por algún problema de seguridad relacionado con los activos. Se estiman tres niveles para cada área: bajo, moderado y alto impacto, cada nivel tiene un valor numérico asignado, 1, 2 y 3 respectivamente.

CRITERIO DE MEDICIÓN DEL RIESGO		Reputación y confianza	
ÁREA DE IMPACTO	**BAJO (1)**	**MODERADO (2)**	**ALTO (3)**
Reputación	La información relacionada con un incidente de seguridad se conoce dentro de la DGRU.	La información relacionada con un incidente de seguridad se conoce entre las entidades y dependencias universitarias con las que se tiene relación.	La información relacionada con un incidente de seguridad se conoce en toda la Universidad y fuera de ella.
Confianza de proveedores de datos y usuarios (investigadores, estudiantes, etc.)	A través de los canales de comunicación se reciben en la dependencia dudas sobre la confiabilidad e integridad de la información que se consulta a través de las plataformas de la DGRU.	Durante los procesos de integración de contenidos, metadatos y repositorios, los posibles proveedores de datos muestran duda o renuencia a integrar su información a las plataformas de la DGRU, derivado de incidentes de seguridad conocidos.	Los usuarios no confían en la DGRU en términos de disponibilidad, confidencialidad o integridad de la información que le proporcionan o que consultan a través de las plataformas de la DGRU, por lo que los proveedores de datos dejan de integrar sus contenidos o la utilización de dichas plataformas se ve reducida.
Confianza del personal que brinda sus servicios	La información relacionada con un incidente de seguridad se conoce solo en un grupo de personas dentro de la DGRU.	La información relacionada con un incidente se conoce entre el personal que brinda servicios a la DGRU y los titulares de la información manifiestan inconformidades sin emprender acciones legales.	La información relacionada con un incidente se conoce dentro y fuera de la DGRU y los titulares de la información inician acciones legales.

CRITERIO DE MEDICIÓN DEL RIESGO		Financiera	
ÁREA DE IMPACTO	**BAJO (1)**	**MODERADO (2)**	**ALTO (3)**
Costos operativos	Se puede solventar con el presupuesto corriente (Sin solicitar presupuesto adicional, sin comprar equipo, sin contratar más personal)	Se requieren recursos adicionales menores al 5% del presupuesto anual	Se requieren recursos adicionales mayores al 5% del presupuesto anual.

CRITERIO DE MEDICIÓN DEL RIESGO			Productividad
ÁREA DE IMPACTO	**BAJO (1)**	**MODERADO (2)**	**ALTO (3)**
Cumplimiento de compromisos institucionales	Las metas comprometidas para el trimestre en curso se entregan con retraso.	Las metas comprometidas para el trimestre en curso y los subsecuentes se entregan con retraso.	Una o más metas anuales no se cumplen.
Disponibilidad de plataformas en línea	La disponibilidad de las plataformas se ve afectada en un plazo menor a 24 horas.	La disponibilidad de las plataformas se ve afectada en un plazo menor a 48 horas.	La disponibilidad de las plataformas se ve afectada en un plazo mayor a 48 horas.
Disponibilidad de plataformas digitales internas o de la información proveída por éstas	La disponibilidad de las plataformas o de la información se ve afectada en un plazo menor a 24 horas.	La disponibilidad de las plataformas o de la información se ve afectada en un plazo menor a 48 horas.	La disponibilidad de las plataformas o de la información se ve afectada en un plazo mayor a 48 horas.

CRITERIO DE MEDICIÓN DEL RIESGO			Seguridad y salud
ÁREA DE IMPACTO	**BAJO (1)**	**MODERADO (2)**	**ALTO (3)**
Salud	Hay un daño mínimo tratable de manera inmediata sin atención hospitalaria.	Hay un daño temporal, tratable con atención hospitalaria.	Hay un daño permanente.
Seguridad	Seguridad cuestionada, sin responsabilidad regulatoria.	Seguridad afectada, mínima responsabilidad regulatoria.	Seguridad violada, responsabilidad regulatoria significativa que implique investigaciones.

CRITERIO DE MEDICIÓN DEL RIESGO			Medidas de apremio y sanciones
ÁREA DE IMPACTO	**BAJO (1)**	**MODERADO (2)**	**ALTO (3)**
Medidas de apremio y sanciones	Amonestación pública de conformidad con LGPDPPPSO. El incumplimiento de los sujetos obligados es difundido en los portales de obligaciones de transparencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y los Organismos garantes y considerados en las evaluaciones que realicen éstos.	Multa de conformidad con la LGPDPPSO. El incumplimiento de los sujetos obligados es difundido en los portales de obligaciones de transparencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y los Organismos garantes y considerados en las evaluaciones que realicen éstos.	Amonestación pública, multas y/o sanciones administrativas en conformidad con la LGPDPPSO y aquellas del orden civil, penal o de cualquier otro tipo que pueda derivar del hecho. El incumplimiento de los sujetos obligados es difundido en los portales de obligaciones de transparencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y los Organismos garantes y considerados en las evaluaciones que realicen éstos.

Los criterios de medición de riesgo priorizados para la DGRU se presentan en orden descendente:

PRIORIDAD DE LAS ÁREAS DE IMPACTO PARA LA DGRU	
PRIORIDAD	**ÁREAS DE IMPACTO**
5	Reputación y confianza
4	Seguridad y salud
3	Productividad
2	Financiera
1	Multas y penas legales

Anexo 12. Medidas de Seguridad Técnicas (MST)

1. RUTA CRÍTICA PARA EL CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS (MST)

Anexo IV de las Normas Complementarias

Dada la complejidad de diversos sistemas en la UNAM, se ha dispuesto la ruta crítica para el cumplimiento de las MST en tres etapas para los sistemas de información que a la fecha de publicación de esta guía estén en producción o funcionamiento. Todo sistema de información deberá satisfacer a cabalidad el 100% de las MST en un tiempo máximo de un año contado a partir de la publicación de las MST para conservar su registro y publicación dentro del dominio institucional .***unam.mx***.

A) **Etapa 1. Corto plazo**. Requisitos de misión crítica y mínimos indispensables para la protección de datos personales y datos personales sensibles. Cumplimiento obligatorio en menos de treinta días hábiles.

B) **Etapa 2. Mediano plazo**. Requisitos importantes para garantizar la protección de datos personales y datos personales sensibles. Ejecución estimada entre un mes y seis meses.

C) **Etapa 3. Largo plazo**. Requisitos necesarios para reforzar la seguridad en la protección de datos personales y datos personales sensibles. Ejecución estimada entre seis y doce meses

Dada la extensión de las medidas técnicas y el número de sistemas involucrados, se concentran en este documento, las acciones realizadas para el cumplimiento de las Medidas de Seguridad Técnicas en términos de los artículos 18, 19 y 20 de las *Normas Complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la universidad* que deben cumplirse, independientemente de los formatos que deben elaborarse por cada activo y para cada artículo como la normatividad lo señala.

2. RELACIÓN DE PLATAFORMAS, INFRAESTRUCTURA Y SERVICIOS RELACIONADOS CON LOS ACTIVOS DEL TRATAMIENTO DE DATOS PERSONALES

[redacted]

ACTIVO	IJ1 Instrumentos jurídicos de la DGRU, PE1 Apoyo de gestión administrativa del personal, DG1 Contraseñas de gestión administrativa, DG2 Formatos de gestión interna DG3 Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos DTI1 Correo electrónico	
PLATAFORMA / SISTEMA	INFRAESTRUCTURA (SERVIDORES)	TIPO DE SERVICIO
[redacted]	[redacted]	[redacted]
		[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

ACTIVO	SRU1 Repositorio Institucional de la UNAM	
PLATAFORMA / SISTEMA	INFRAESTRUCTURA (SERVIDORES)	TIPO DE SERVICIO
[redacted]	[redacted]	[redacted]

		[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

ACTIVO	CDI1 Portal de Datos Abiertos UNAM, Colecciones Universitarias	
PLATAFORMA / SISTEMA	**INFRAESTRUCTURA (SERVIDORES)**	**TIPO DE SERVICIO**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

		[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

ACTIVO	DTI2 Cámaras de seguridad	
PLATAFORMA / SISTEMA	INFRAESTRUCTURA (SERVIDORES)	TIPO DE SERVICIO
[redacted]	[redacted]	[redacted]

3. ETAPA 1 - ARTÍCULO 18.I. c): UTILIZAR DATOS NO PERSONALES DURANTE EL DESARROLLO Y PRUEBAS DE LOS SISTEMAS

Repositorio Institucional de la UNAM			SRU1	
Formato	**1**	**Verificación anual**	**Acción concluida**	[redacted]
Medida de seguridad técnica:	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.			

Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.

Ejecución	**Fecha inicio**
[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Nombre y firma Programador, desarrollador o diseñador del sistema de información	Fecha término [redacted]
Observaciones / anotaciones	[redacted]

Portal de Datos Abiertos UNAM, Colecciones Universitarias			CDI1	
Formato	**1**	**Verificación anual**	**Acción concluida**	[redacted]
Medida de seguridad técnica:	**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			

Tiempo estimado:	Un día hábil.
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Ejecución	Fecha inicio
[redacted]	[redacted]
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

[redacted]

4. ETAPA 1 - ARTÍCULO 18.I. e): ASIGNAR O REVOCAR LOS PRIVILEGIOS DE ACCESO PARA LOS USUARIOS TENIENDO COMO BASE EL PRINCIPIO DEL MENOR PRIVILEGIO

Plataforma de almacenamiento de archivos (Activos: Instrumentos jurídicos de la DGRU; Apoyo de gestión administrativa del personal; Contraseñas de gestión administrativa; Formatos de gestión interna; Grabaciones y formatos de autorización para el uso de imagen o voz personales y contenidos; Correo electrónico			IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			

Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.

Ejecución	**Fecha inicio**
[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Nombre y firma Programador, desarrollador o diseñador del sistema de información	Fecha término [redacted]
Observaciones / anotaciones	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Repositorio Institucional de la UNAM			SRU1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.			

	D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término** [redacted]

Observaciones / anotaciones	[redacted]

Portal de Datos Abiertos UNAM, Colecciones Universitarias			**Identificador único** CDI1	
Formato:	**2**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			

Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.

Ejecución	**Fecha inicio**

[redacted]	[redacted]
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

Cámaras de seguridad			Identificador único DTI2	
Formato:	**2**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.			

	D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.
Mejores prácticas, referencias:	**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Programador, desarrollador o diseñador del sistema de información	**Fecha término** [redacted]

Observaciones / anotaciones	[redacted]

5. ETAPA 1 - ARTÍCULO 18.I. g): INSTALAR Y MANTENER VIGENTES CERTIFICADOS DE COMUNICACIÓN SEGURA SSL EN EL CASO DE SERVICIOS BASADOS EN WEB

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**3**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			

Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.
Proceso recomendado:	**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.
Mejores prácticas, referencias:	**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (wildcard). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.

Ejecución	**Fecha inicio**

[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

6. ETAPA 1 - ARTÍCULO 18.I. h): DEFINIR EL PLAN DE RESPALDOS DE LA INFORMACIÓN, INCLUYENDO PERIODICIDAD Y ALCANCE

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1
Plataforma de almacenamiento de archivos	IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Formato:	**4**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.			
Proceso recomendado:	**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:			

	- En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: Recovery Time Objective. Tiempo objetivo de recuperación. - RPO: Recovery Point Objective: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Ejecución	Fecha inicio
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

7. ETAPA 1 - ARTÍCULO 18.I. i): DEFINIR EL PROCEDIMIENTO PARA EL BORRADO SEGURO

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**5**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.			

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Proceso recomendado:	**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar DOD-5220.22-M.
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.

Ejecución	**Fecha inicio**

[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

8. ETAPA 1 - ARTÍCULO 18.II. a): SINCRONIZAR LA FECHA Y HORA CON EL SERVIDOR NTP (NETWORK TIME PROTOCOL) OFICIAL DE LA UNAM

Repositorio Institucional de la UNAM	SRU1

Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**6**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.			
Proceso recomendado:	**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo.			

	B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. Por ejemplo, en el caso del sistema operativo Linux: - Verificar la existencia del archivo /etc/ntp.conf - Editar el archivo ntp.conf incluyendo en la primera línea: server ntpdgtic.redunam.unam.mx ó server 132.247.169.17 - Reiniciar el demonio del cliente NTP con el comando sudo service ntp reload. **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.
Conocimientos requeridos:	Administración de sistema operativo.

Ejecución	Fecha inicio
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

9. ETAPA 1 - ARTÍCULO 18.II. b): INSTALAR Y MANTENER ACTUALIZADOS EL SOFTWARE ANTIMALWARE

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1
Plataforma de almacenamiento de archivos	

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

			IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	7	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de malware (rootkits, backdoors o códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:		**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. Por ejemplo, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como chkrootkit, rootkit hunter, bothunter, clamAV, avast, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso.		

	B) Disponer de comandos para la localización de amenazas. Por ejemplo, para el caso de Linux, se recomienda usar el comando grep para la detección de cadenas regulares de texto en las invocaciones al shell. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** UNAM-CERT puede asesorar en la selección de las herramientas anti malware más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]

Observaciones / anotaciones	[redacted]

10. ETAPA 1 - ARTÍCULO 18.II. c): INSTALAR LAS ACTUALIZACIONES DE SEGURIDAD MÁS RECIENTES DISPONIBLES

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**8**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**			

Aplicable en:	II. Sistemas operativos y servicios.
Tiempo estimado:	Cuatro días hábiles.
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.
Proceso recomendado:	**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. Por ejemplo, en el sistema operativo Linux ejecutar apt-get update para obtener la lista de actualizaciones, especialmente en el repositorio security de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	1.- Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.

Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]

Observaciones / anotaciones	[redacted]

11. ETAPA 1 - ARTÍCULO 19.I. a): APLICAR UN MECANISMO DE AUTENTICACIÓN PARA LAS PERSONAS AUTORIZADAS CON BASE EN EL PRINCIPIO DEL MENOR PRIVILEGIO

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**9**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Cuatro días hábiles.			

Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.
Proceso recomendado:	**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. Por ejemplo: el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **C)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (Active Directory), LDAP u OpenAIM. **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.

Ejecución	**Fecha inicio**

[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

12. ETAPA 1 - ARTÍCULO 19.II. b): EVITAR LA INSTALACIÓN DE CUALQUIER ELEMENTO DE SOFTWARE QUE IMPLIQUE ALGÚN RIESGO PARA EL TRATAMIENTO DE DATOS PERSONALES

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**10**	**Verificación anual**	**Acción concluida**	[redacted]
Medida de seguridad técnica:	**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Dos días hábiles.			

Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.
Proceso recomendado:	**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. Por ejemplo: en sistemas Linux desactivar la instalación de versiones beta, test, debug, non-official. **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones TSR (Terminal and Stay Resident). Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. Por ejemplo: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. Por ejemplo, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio dchpd no debe estar instalado. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.

Ejecución	Fecha inicio
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

13. ETAPA 1 - ARTÍCULO 19.III. a): ESTABLECER LAS MEDIDAS FÍSICAS DE SEGURIDAD QUE CONTROLEN EL ACCESO A LOS EQUIPOS

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Plataforma de almacenamiento de archivos Cámaras de seguridad			IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**11**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.			
Proceso recomendado:	**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar.			

	C) Establecer y seguir un plan de mejoramiento de la protección física de equipos. Por ejemplo; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte del plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]

Observaciones / anotaciones	[redacted]

14. ETAPA 1 - ARTÍCULO 19.III. b): RESTRINGIR LA SALIDA DE EQUIPOS DE LAS INSTALACIONES DE CADA ÁREA UNIVERSITARIA

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**12**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**			

Aplicable en:	III. Equipo de cómputo.
Tiempo estimado:	Un día hábil.
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.
Proceso recomendado:	**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades flash, discos ópticos, monitores, teclados, ratones y en general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]

Observaciones / anotaciones	[redacted]

15. ETAPA 1 - ARTÍCULO 19.IV. a): REALIZAR LA TRANSMISIÓN DE DATOS PERSONALES A TRAVÉS DE UN CANAL CIFRADO

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**13**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:		**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Tres días hábiles.		

Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.
Proceso recomendado:	**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. Por ejemplo: SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. Por ejemplo, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando apt-get install openssh-server. **C)** Activar los protocolos de comunicación encriptada en el servidor. Por ejemplo: en Linux con el comando sudo systemctl enable ssh. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. **2.-** El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.

Ejecución	Fecha inicio
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

16. ETAPA 1 - ARTÍCULO 20: APLICAR EL PROCEDIMIENTO DE BORRADO SEGURO QUE IMPIDA LA RECUPERACIÓN EN LAS BASES DE DATOS Y TODOS SUS RESPALDOS

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1

Formato:	**14**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**			
Aplicable en:	Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).			
Proceso recomendado:	**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. Por ejemplo: máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa.			

	D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. Por ejemplo: en Linux se dispone de shred, wipe, secure-delete, srm, sfill, sswap, sdmem, que se pueden instalar desde el administrador de aplicaciones. **E)** Llenar y firmar este formato.
Mejores prácticas, referencias:	**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]

Observaciones / anotaciones	[redacted]

17. ETAPA 2 - ARTÍCULO 18.I. a): UTILIZAR LOS DATOS PERSONALES PREEXISTENTES QUE ESTÉN DISPONIBLES, DE ACUERDO CON SUS RESPECTIVAS POLÍTICAS DE USO Y ACCESO, EN BASES DE DATOS A CARGO DE OTRAS ÁREAS UNIVERSITARIAS

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias			SRU1 CDI1	
Formato:	**15**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas	**Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			

Tiempo estimado:	Hito.
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.
Proceso recomendado:	**A)** Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas. **B)** Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. *Por ejemplo*: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes. **C)** Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa. **D)** Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. *Por ejemplo*: *Webservices*, transferencia *SFTP*. **E)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.
Ejecución	**Fecha inicio**

[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

NOTA: Esta Medida de Seguridad Técnica no aplica para la plataforma de almacenamiento de archivos box.ccud.unam.mx, ni para el Sistema interno de videovigilancia.

18. ETAPA 2- ARTÍCULO 18.I. d): PERMITIR EL ACCESO AL CÓDIGO FUENTE DE LOS SISTEMAS EXCLUSIVAMENTE A LA ADMINISTRACIÓN DEL SISTEMA Y PERSONAL PARA EL DESARROLLO

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1

Formato:	**16**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.			

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Mejores prácticas, referencias:	**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]
Observaciones / anotaciones	[redacted]

19. ETAPA 2- ARTÍCULO 19.I. b): ESTABLECER LAS MEDIDAS DE SEGURIDAD EN LOS PERIODOS DE INACTIVIDAD O MANTENIMIENTO

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**17**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.
Proceso recomendado:	**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.

Ejecución	**Fecha inicio**
[redacted]	[redacted]

Nombre y firma Administrador del sistema de información o servidor	Fecha término [redacted]
Observaciones / anotaciones	[redacted]

20. ETAPA 2- ARTÍCULO 19.I. c): GENERAR RESPALDOS Y APLICAR LOS MECANISMOS DE CONTROL Y PROTECCIÓN PARA SU RESGUARDO

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**18**	**Verificación anual**	**Acción concluida**	[redacted]

Medidas de seguridad técnica:	**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**
Aplicable en:	I. Bases de datos y sistemas de tratamiento.
Tiempo estimado:	Ocho días hábiles.
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.
Proceso recomendado:	**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]

Observaciones / anotaciones	[redacted]

	[redacted]

21. ETAPA 2 - ARTÍCULO 19.I. d): IMPEDIR EL USO DE CUENTAS Y SERVICIOS GESTIONADOS POR PERSONAS FÍSICAS PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**19**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**			

Aplicable en:	I. Bases de datos y sistemas de tratamiento.
Tiempo estimado:	Veinte días hábiles.
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.
Proceso recomendado:	**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx **D)** Llenar y firmar formato.
Mejores prácticas,	**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control

referencias:	dependa de una sola persona.
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término**
	[redacted]

Observaciones / anotaciones	[redacted]

22. ETAPA 2 - ARTÍCULO 19.II. a): PROTEGER ANTE MANIPULACIONES INDEBIDAS Y ACCESOS NO AUTORIZADOS LAS BITÁCORAS Y LOS DISPOSITIVOS DONDE SE ALMACENAN

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**20**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Cuatro días hábiles.			

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.
Proceso recomendado:	**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.

Ejecución	**Fecha inicio**
	[redacted]

[redacted]	
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

23. ETAPA 2 - ARTÍCULO 19.IV. b): SUPERVISAR LOS CONTROLES DE SEGURIDAD EN LA RED DE DATOS DONDE OPERE EL SISTEMA PARA TRATAMIENTO DE DATOS PERSONALES

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Plataforma de almacenamiento de archivos Cámaras de seguridad			IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**21**	**Verificación anual**	**Acción concluida**	[redacted]
Norma Complementaria Técnica	**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.			
Proceso recomendado:	**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones.			

	B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **F)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.
Conocimientos requeridos:	Administración de redes de datos.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma	**Fecha término**

Administrador del sistema de información o servidor	[redacted]
Observaciones / anotaciones	[redacted]

24. ETAPA 2 - ARTÍCULO 19.IV. c): PROPORCIONAR EXCLUSIVAMENTE EL ACCESO DESDE REDES Y SERVICIOS AUTORIZADOS

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1
Plataforma de almacenamiento de archivos	IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1
Cámaras de seguridad	DTI2

Formato:	**22**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Es necesario reducir al mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.			
Proceso recomendado:	**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema.			

	D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]

Observaciones / anotaciones	[redacted]

25. ETAPA 3 - ARTÍCULO 18.I. b): CONTAR CON ENTORNOS PARA DESARROLLO, PRUEBAS Y OPERACIÓN

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias			SRU1 CDI1	
Formato:	**23**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.
Proceso recomendado:	**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.

Ejecución	**Fecha inicio**
[redacted]	[redacted]

Nombre y firma Administrador del sistema de información o servidor	Fecha término [redacted]
Observaciones / anotaciones	[redacted]

26. ETAPA 3- ARTÍCULO 18.I. f): CUMPLIR CON LAS ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA PREVIO A LA PUESTA EN OPERACIÓN

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias			SRU1 CDI1	
Formato:	**24**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			

Tiempo estimado:	Veinte días hábiles.
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .
Proceso recomendado:	**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.

Ejecución	**Fecha inicio**
[redacted]	[redacted]

Nombre y firma Administrador del sistema de información o servidor	Fecha término [redacted]
Observaciones / anotaciones	[redacted]

27. ETAPA 3- ARTÍCULO 18.III. a): UTILIZAR EQUIPOS CON COMPONENTES ACTUALIZADOS, PROTEGIDOS CON GARANTÍAS Y SOPORTE, Y CON LA CAPACIDAD SUFICIENTE PARA ATENDER LA DEMANDA DEL SERVICIO Y DE LOS USUARIOS

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**25**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**			

Aplicable en:	III. Equipos de cómputo.
Tiempo estimado:	Hito.
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.
Proceso recomendado:	**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** El mantenimiento preventivo debe contar con medidas de verificación.
Conocimientos requeridos:	Administración de infraestructura.

Ejecución	Fecha inicio
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

28. ETAPA 3- ARTÍCULO 18.III. b): DEFINIR EL PROGRAMA DE MANTENIMIENTO PREVENTIVO

Repositorio Institucional de la UNAM	SRU1
Portal de Datos Abiertos UNAM, Colecciones Universitarias	CDI1
Plataforma de almacenamiento de archivos	IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Formato:	**26**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:		**Artículo 18. III. b) Definir el programa de mantenimiento preventivo.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento. **B)** En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico. **C)** Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y		

	reemplazos.
Conocimientos requeridos:	Administración de infraestructura.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

29. ETAPA 3 - ARTÍCULO 19.III. c): APLICAR EL PROGRAMA DE MANTENIMIENTO PREVENTIVO A LOS EQUIPOS

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1	
Formato:	**27**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza			

	respectivo. **C)** Llenar y firmar formato.
Mejores prácticas, referencias:	**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.
Conocimientos requeridos:	Administración de infraestructura.

Ejecución	**Fecha inicio**
[redacted]	[redacted]
Nombre y firma Administrador del sistema de información o servidor	**Fecha término** [redacted]
Observaciones / anotaciones	[redacted]

	[redacted]

30. ETAPA 3 - ARTÍCULO 21: SOLO SE PERMITIRÁ EL USO DE SERVICIOS DE NUBE PÚBLICA PARA EL RESGUARDO DE ARCHIVOS CIFRADOS QUE CONTENGAN RESPALDOS DE LA INFORMACIÓN

Repositorio Institucional de la UNAM Portal de Datos Abiertos UNAM, Colecciones Universitarias Plataforma de almacenamiento de archivos Cámaras de seguridad			SRU1 CDI1 IJ1 - PE1 - DG1 - DG2 - DG3 - DTI1 DTI2	
Formato:	**28**	**Verificación anual**	**Acción concluida**	[redacted]
Medidas de seguridad técnicas:	**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**			

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Aplicable en:	Servicios en la nube pública.
Tiempo estimado:	Hito.
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.
Proceso recomendado:	**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.
Mejores prácticas, referencias:	**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.

Ejecución	**Fecha inicio**
[redacted]	[redacted]

DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

Nombre y firma Administrador del sistema de información o servidor	Fecha término [redacted]
Observaciones / anotaciones	[redacted]

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

Visto el expediente relativo a la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública, que someten la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado** y la **Dirección General de Asuntos Jurídicos,** en relación con sus respectivos **Documentos de Seguridad**, se procede a dictar la presente resolución con base en los siguientes:

A N T E C E D E N T E S

I. Con fecha 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.

II. Mediante Acuerdo **ACT-PUB/19/12/2017.10**, de fecha 19 de diciembre de 2017, publicado en el Diario Oficial de la Federación con fecha 26 de enero de 2018, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. A través del Acuerdo **ACT-PUB/11/11/2020.05**, de fecha 11 de noviembre de 2020, publicado en el Diario Oficial de la Federación con fecha 25 de noviembre de 2020, dicho Órgano Garante aprobó la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público, a fin de establecer las disposiciones generales que permitirán desarrollar el procedimiento de diseño y aplicación del sistema y procedimiento para llevar a cabo la evaluación sobre el desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia.

IV. Por Acuerdo **ACT-PUB/17/11/2021.05**, de fecha 17 de noviembre de 2021, publicado en el Diario Oficial de la Federación con fecha 26 de noviembre de 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó los "Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados".

V. Los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como las reglas Décima Tercera y Décima Cuarta del apartado "V. Reglas de Generales de Evaluación" del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que la información y documentos que se pongan a disposición de los titulares de datos personales y del Instituto, deberán ser revisados por el responsable a fin de verificar que no contengan información confidencial o reservada y, de ser el caso, deberá publicarse la versión pública de dicha documentación.

Por otra parte, en el apartado "VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia", Capítulo II. Criterios y formatos, **Vertiente 2**: Deberes, **Variable 2.1** Deber de seguridad, se establece que el responsable, por ningún motivo, debe publicar el documento de seguridad de manera íntegra, por lo que deberá poner a disposición la versión pública del mismo, en la cual se deberá proteger la información relativa al plan de trabajo, el análisis de riesgo y el análisis de brecha.

VI. En términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 34, fracción II del Reglamento de Transparencia y Acceso a la Información Púbica de la Universidad Nacional Autónoma de México, la clasificación de la información será procedente cuando, entre otros supuestos, se determiné mediante una resolución de autoridad competente.

VII. Mediante oficio **CSAMorelos/533.01/0289/2022**, recibido fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Servicios Administrativos Morelos,** informó lo siguiente:

> *"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[1]; exige elaborar versión pública del documento de seguridad de esta área universitaria.*
>
> *Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.*

[1] *DOF: 26 de noviembre de 2021*

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obra en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados, cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*16 -40*
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*16 -40*
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*16 -40*

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riego real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de

diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

VIII. Mediante oficio **CVTT/038/2022**, recibido fecha 18 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación de Vinculación y Transferencia Tecnológica** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[2]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad

[2] *DOF: 26 de noviembre de 2021*

técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
Anexo 1. Inventario de sistemas de tratamiento de datos personales	*El inventario de los sistemas de tratamiento de datos personales contiene información sobre las rutas de acceso a soportes digitales de la información y cuentas, los cuales pueden ser utilizados para un ataque informático a los activos críticos y no críticos.*	*12-95*
Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales	*La estructura y descripción de los sistemas de tratamiento de datos personales contiene información sobre las rutas y métodos de acceso a soportes digitales y físicos de la información, los cuales pueden ser utilizados para un ataque a los activos críticos y no críticos.*	*97-128*
Anexo 3. Diagramas de arquitectura	*Los diagramas de arquitectura de los soportes digitales contienen el flujo de información entre los componentes, sus rutas de acceso a soportes digitales y describe las medidas de seguridad implementadas, información que puede ser utilizada para un ataque informático a los activos críticos y no críticos.*	*130-156*

Anexo 5. Análisis de riesgos y análisis de brecha	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.* *El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*270-381*
Anexo 6. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*383-389*

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos*

controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

- *En este sentido la revelación de la información que obra el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, el análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha, las políticas de respaldo y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a

que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

IX. Mediante oficio **ET/DGTIC/040/2022**, recibido con fecha 19 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Cómputo y Tecnologías de Información y Comunicación** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[3]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos

[3] *DOF: 26 de noviembre de 2021*

Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta dependencia universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva … se solicita a ese Comité de la siguiente forma:

Reserva total o parcial	***Anexos o Políticas***	***Contenido y su afectación***	***Páginas***
Reserva Parcial	***a)*** *Inventario de datos personales*	*El inventario contiene información técnica y operativa que permite identificar los espacios físicos e infraestructura tecnológica en que se resguardan datos personales*	*19 de 47*
Reserva Total	***b)*** *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*63*
Reserva Total	***c)*** *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*20*
Reserva Total	***d)*** *Plan de Trabajo y Medidas de Seguridad.*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*1*
Reserva	***e)*** *Política de*	*Las políticas contienen información*	*4*

Total	*autenticación y control de acceso*	*del conjunto de reglas diseñadas para determinar a quién se le concede acceso a un lugar restringido o a una información restringida relacionada con los datos personales en posesión de la dependencia.*	
Reserva Total	***f)** Política de seguridad física y ambiental*	*Las políticas contienen información sobre las medidas que se adoptarán para proteger los sistemas, los edificios y la infraestructura de apoyo de los sistemas de datos personales contra las amenazas asociadas con ambiente físico.*	*4*

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en el inventario de datos personales, análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de seguridad física y ambiental y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el inventario de datos personales, análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de seguridad física y ambiental y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el inventario de datos personales, análisis de riesgo, el análisis de brecha las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y el plan de trabajo de esta dependencia universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta dependencia, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al inventario de datos personales, análisis de riesgo, al análisis de brecha, las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y al plan de trabajo de esta dependencia se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva parcial del inventario de datos personales, y la reserva total del análisis de riesgo, el análisis de brecha, las políticas de autenticación y control de acceso, así como de Seguridad física y ambiental y el plan de trabajo cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta dependencia universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento

de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

X. Mediante oficio **DGRU/DG/090/2022/am** recibido con fecha 19 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Repositorios Universitarios** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[4]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

[4] *DOF: 26 de noviembre de 2021*

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) *Análisis de riesgos*	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*Anexo 1. 38-44* *Anexo 2. 91-101* *Anexo 3. 154-163* *Anexo 4. 201-210* *Anexo 5. 254-266* *Anexo 6. 317-329* *Anexo 7. 377-393* *Anexo 8. 437-457* *Anexo 9. 514-529* *Anexo 10. 579-586*
b) *Análisis de brecha*	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*Anexo 1. 45-48* *Anexo 2. 101-106* *Anexo 3. 163-165* *Anexo 4. 210-214* *Anexo 5. 266-270* *Anexo 6. 329-332* *Anexo 7. 393-398* *Anexo 8. 457-462* *Anexo 9. 529-533* *Anexo 10. 586-589*
c) *Plan de Trabajo*	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*Anexo 1. 49-50* *Anexo 2. 106-108* *Anexo 3. 165* *Anexo 4. 214-215* *Anexo 5. 270-272* *Anexo 6. 333-334* *Anexo 7. 398-399* *Anexo 8. 462-465* *Anexo 9. 534-536* *Anexo 10. 589-590*
d) *Políticas de Respaldos*	*Las políticas de respaldo contienen información del momento que se hacen los respaldos, así como la ubicación física de estos, que podrían ocasionar la pérdida, destrucción no autorizada, robo, copia no autorizada, uso, acceso o tratamiento no autorizado, el daño la alteración o modificación no autorizada de datos personales.*	*Anexo 1. 65-66* *Anexo 2. 127-128* *Anexo 3. 182-183* *Anexo 4. 230-232* *Anexo 5. 287-289* *Anexo 6. 352-354* *Anexo 7. 412-413* *Anexo 8. 486-488* *Anexo 9. 557-560* *Anexo 10. 604-606*
e) *Medidas de Seguridad*	*Las medidas de seguridad técnicas contienen las acciones implementadas o por implementar para proteger los datos*	*Anexo 12. 618-705*

Técnicas	*personales que se encuentren en formato digital, así como de los sistemas informáticos que les dan tratamiento.*	

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha, las políticas de respaldo, el plan de trabajo y medidas de seguridad técnicas de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

XI. Mediante oficio **DGCS/016/2022**, recibido fecha 22 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Comunicación Social** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[5]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

[5] *DOF: 26 de noviembre de 2021*

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	
c) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de*	

	brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.	

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planeamos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

XII. Mediante oficio **ICML/DIR/241/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, el **Instituto de Ciencias del Mar y Limnología** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[6]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

[6] *DOF: 26 de noviembre de 2021*

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
Anexo 1. Inventario de sistemas de tratamiento de datos personales	*Se testaron algunas partes del inventario de los sistemas de tratamiento de datos personales, las cuales contienen información sobre las rutas de acceso a soportes digitales de la información y cuentas, los cuales pueden ser utilizados para un ataque informático a los activos críticos y no críticos.*	*11, 13, 26 y 36*
Anexo 2. Estructura y descripción de los sistemas de tratamiento de datos personales	*Se testaron algunas partes de la estructura y descripción de los sistemas de tratamiento de datos personales, las cuales contienen información sobre las rutas y métodos de acceso a soportes digitales y físicos de la información y la descripción y características de los lugares de resguardo, los cuales pueden ser utilizados para un ataque a los activos críticos y no críticos. Adicionalmente, los diagramas de arquitectura contenidos en dicho anexo contienen flujo de*	*43-49*

	información entre los componentes, sus rutas de acceso a soportes digitales y describe las medidas de seguridad implementadas, información que poder ser utilizada para un ataque informático a los activos críticos y no críticos.	
Anexo 3. Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*50-66*
Anexo 4. Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*67-96*
Anexo 5. Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*97-98*

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha ... y el plan de trabajo de esta dependencia evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

- *En este sentido la revelación de la información que obra el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha … y el plan de trabajo de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al inventario, estructura y descripción de los sistemas de tratamiento de datos personales, diagramas de arquitectura, análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica

negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

XIII. Mediante oficio **CGEP/0493/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Coordinación General de Estudios de Posgrado** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[7]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el

[7] *DOF: 26 de noviembre de 2021*

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Estructura y descripción de los sistemas de tratamiento de datos personales	*La estructura y descripción de los sistemas de tratamiento de datos personales, refiere especificidades de cada uno de los sistemas a cargo de esta área, como son: la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo. El uso de esta información podría ocasionar ataques informáticos dirigidos particularmente a los sistemas que resguarden el catálogo de datos personales que resulten de mayor interés para la comisión de un ilícito.*	*16 a 18*
b) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*18 a 20*
c) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*20*
d) Plan de Trabajo	*El plan de trabajo define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento que se implementen nuevos controles.*	*21*

e) Medidas de seguridad implementadas	*Con las medidas de seguridad se darían a conocer aspectos relacionados con los sistemas e infraestructura con los que cuenta esta área universitaria, así como el dictamen del análisis de vulnerabilidades de la información en los que se enuncian el inventario de sistemas, puertos de comunicación, versiones y características de las comunicaciones y equipos integrados a la red de datos, e incluso los mecanismos de seguridad y de control de la información.*	*21 a 25*
f) Mecanismos de monitoreo y revisión de medidas de seguridad	*Los mecanismos de monitoreo y revisión de medias de seguridad indican las herramientas que son utilizadas para el monitoreo de la protección de datos, así como la periodicidad en la que se realiza la revisión correspondiente, por lo que, existe un riesgo en que dicha información se utilizada para que a través de ingeniería inversa o procesos análogos se tenga acceso a los sistemas de tratamiento de datos personales.*	*25*

Los fundamentos y motivos se exponen a continuación:

- *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riesgo real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

- *Divulgar los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de*

seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.

- *En este sentido la revelación de la información que obra en los apartados consistentes en la estructura y descripción de los sistemas de tratamiento de datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, las medidas de seguridad implementadas en esta dependencia y los mecanismos de monitoreo y revisión de dichas de seguridad, revelan y hacen identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta área para reaccionar ante posibles amenazas.*

La prueba de daño precitada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha y el plan de trabajo de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta Área Universitaria, con relación al cumplimiento de los principios de protección de datos personales previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha y al plan de trabajo de esta área se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales de no solo la comunidad universitaria sino de cualquiera que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva de cada uno de esos apartados que obran en el documento de seguridad de esta área universitaria (anexo), por un periodo de 5 años, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

XIV. Mediante oficio **DGAJ/SP/DCS/6577/2022**, recibido con fecha 23 de agosto del 2022, dirigido a la Presidencia del Comité de Transparencia, la **Dirección General de Asuntos Jurídicos** informó lo siguiente:

"Los Instrumentos Técnicos a los que se refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público en materia de evaluación del desempeño de los sujetos obligados del sector público federal en el cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[8]; exige elaborar versión pública del documento de seguridad de esta área universitaria.

Una vez analizada la información que se solicitó en el primer punto del 'Documento de seguridad', se observó que la misma se ajusta al supuesto de reserva contemplado en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, ya que su divulgación obstruiría el deber de esta Universidad de establecer y mantener las medidas de seguridad técnica, administrativa y física de los datos personales que los titulares confían a esta institución.

En este contexto, la información puede ser clasificada como reservada en términos de los artículos 106, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública (Ley General) y 98 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública (Ley Federal), en relación con los artículos 247 y 248 de Lineamientos Generales de Protección de Datos Personales para el Sector Público y las reglas generales de evaluación Décima Tercera y Décima Cuarta del apartado V. Reglas de Generales de Evaluación, del Documento Técnico de Evaluación y sus anexos de los Instrumentos Técnicos que refiere el Título Décimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en materia de Evaluación del Desempeño de los Sujetos Obligados del Sector Público Federal en el Cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

A efecto de cumplir con lo señalado, se realiza la siguiente prueba de daño relativa al documento de seguridad de datos personales que obran en el Sistema de Gestión

[8] *DOF: 26 de noviembre de 2021*

de Seguridad de Datos Personales de esta área universitaria. El documento de seguridad contiene los siguientes apartados cuya autorización de reserva total se solicita a ese Comité:

Anexos o Políticas	***Contenido y su afectación***	***Páginas***
a) Análisis de riesgos	*El análisis de riesgos contiene información sobre las vulnerabilidades de la infraestructura tecnológica de esta área universitaria, y otorga herramientas a las personas para implementar un ataque informático a los activos críticos y no críticos.*	*Numeral 3, páginas 77 a 89.*
b) Análisis de brecha	*El análisis de brecha integra información relativa a la seguridad de la infraestructura tecnológica; enlistan los controles de seguridad con los que cuenta esta área; y menciona las herramientas que se deben adquirir para garantizar un nivel más alto de seguridad de los sistemas de información.*	*Numeral 4, páginas 90 a 93.*
c) Plan de Trabajo y Medidas de seguridad que hagan evidente vulnerabilidades	*El plan de trabajo y las medidas de seguridad que hagan evidente vulnerabilidades, definen los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo real detectado. El uso de esta información permite inferir nuestros riesgos, por cuánto tiempo seguirán así hasta el momento en que se implementen nuevos controles.*	*Numeral 5, páginas 94 a 99 y numeral 6, fracción I, páginas 100 y 101, fracción III, numerales 1, 2, 3, 4, 5 y 6 páginas 102 y 103, fracción IV, numeral 3, cuatro líneas de la página 104, fracción V, numeral 2, página 105,*

		fracciones VII, VIII y IX, página 106.

Los fundamentos y motivos se exponen a continuación:

I. *Existe un riesgo real, demostrable e identificable en perjuicio del nexo causal que prevé la hipótesis de reserva ahora analizada contemplada en los artículos 113, fracción VII, y 110, fracción VII, de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, respectivamente, pues los documentos consistentes en análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad de esta dependencia universitaria contienen información de cómo se protegen los datos personales de los titulares que nos confiaron su información personal y que es nuestra responsabilidad garantizar. Es un riego real el hecho de que toda persona que quiera ocasionar la pérdida, destrucción, robo, copia, uso, acceso o tratamiento no autorizado, daño, alteración o modificación no autorizada de datos personales, puede hacerlo si cuenta con la información exacta de las vulnerabilidades de un área universitaria, lo que esta serie de documentos les otorga directamente si se difundiera la información.*

II. *Divulgar el análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad de esta dependencia universitaria evidencian los nuevos controles que estamos pendientes de implementar, describen la forma en cómo almacenamos técnicamente los datos personales, cómo protegemos los sistemas automatizados de información, qué medidas de seguridad administrativas, físicas y técnicas planemos establecer de manera gradual y de conformidad con las prioridades y presupuestos otorgado.*

III. *En este sentido la revelación de la información que obra el análisis de riesgo, el análisis de brecha … así como el plan de trabajo y las medidas de seguridad de esta área revela y hace identificable las formas en que es posible atacar o vulnerar nuestros sistemas de información que resguardan datos personales que obran en nuestros archivos y dejaría imposibilitada a esta Dirección General para reaccionar ante posibles amenazas.*

La prueba de daño señalada, además de colmar los extremos establecidos en los numerales 97 y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública, en relación con el 104 de la Ley General de Transparencia y Acceso a la Información Pública; también se realiza de conformidad con el Vigésimo Sexto de los Lineamientos Generales en materia de Clasificación y Desclasificación de la Información así como para la elaboración de versiones públicas, donde se prevé que podrá considerarse como información reservada, aquélla que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.

En esa inteligencia, el dar a conocer el análisis de riesgo, el análisis de brecha, así como el plan de trabajo y las medidas de seguridad de esta área universitaria, no podrían prevenirse actos ilícitos que pudieran realizarse en contra de los sistemas de información y tratamiento de datos personales, así como en contra de los activos e infraestructura crítica de esta dependencia; por lo que es posible advertir que algunas de las posibles consecuencias de divulgar dicha información podrían derivar en la comisión de diversos delitos tipificados en el Código Penal Federal, como accesos no autorizados a los sistemas, robos de información, suplantación de identidades, entre otros. Es decir, se advierte que la negativa de acceso a la información se motiva en evitar o prevenir la comisión del delito al vulnerar las medidas de seguridad establecidas por esta área universitaria, con relación al cumplimiento de los principios de protección de datos personales previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En tal sentido, proteger la información de los documentos relativos al análisis de riesgo, al análisis de brecha, así como al plan de trabajo y a las medidas de seguridad de esta área universitaria, se adecua al principio de proporcionalidad porque se justifica negar su divulgación, toda vez que la pretensión de fondo que persigue la reserva de la información consiste en prevenir las conductas antijurídicas tipificadas, aunado a que la restricción es temporal, hasta en tanto las medidas tomadas caduquen; de igual manera, con la no divulgación de la información se contribuye a garantizar la protección de los datos personales no solo de la comunidad universitaria sino de cualquier persona que ponga la confianza en esta Universidad para resguardar sus datos personales.

Por tales motivos, respetuosamente, se propone la reserva total de cada uno de esos documentos, que obran como anexos y políticas del documento de seguridad de esta área universitaria, por un periodo de ***cinco (5) años****, de conformidad con los artículos 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.*

En virtud de lo anterior, le solicito de la manera más atenta que ese Cuerpo Colegiado tenga a bien emitir la resolución que en derecho corresponda …" (sic).

Establecidos los antecedentes del presente asunto, este Comité procede al análisis de los argumentos referidos con antelación, al tenor de las siguientes:

C O N S I D E R A C I O N E S

PRIMERA. Con fundamento en lo dispuesto por los artículos 10 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, así como 8, fracción VI del Reglamento de Responsabilidades Administrativas de las y los Funcionarios y Empleados de la Universidad Nacional Autónoma de México, este Órgano Colegiado rige su funcionamiento, entre otros, bajo los principios de imparcialidad, certeza, legalidad, objetividad y

profesionalismo. Por ello, al ser un asunto propuesto, entre otras Áreas Universitarias, por la **Dirección General de Asuntos Jurídicos**, dependiente de la Oficina de la Abogacía General, en este acto el Abogado General y Presidente del Comité de Transparencia, Alfredo Sánchez Castañeda, así como el Director General de Asuntos Jurídicos y Secretario Técnico de este Comité, Lic. Jorge Barrera Gutiérrez, formalmente se excusan de conocer del caso, para no afectar la imparcialidad del mismo.

SEGUNDA. De conformidad con lo dispuesto en los artículos 1, 10 y 15, fracción X del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, el Comité de Transparencia de la Universidad Nacional Autónoma de México es competente para analizar la clasificación de reserva total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** y determinar, en consecuencia, si la confirma, modifica o revoca.

TERCERA. De conformidad con lo dispuesto en los artículos 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como 33 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, **los titulares de las Áreas Universitarias son responsables de clasificar la información que obre en sus archivos**, debiendo comunicar al Comité mediante oficio, de forma fundada y motivada, esa clasificación.

En tal virtud la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** clasificaron como información reservada, por un periodo de **cinco años**, la relativa: al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos, así como las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**; lo anterior, conforme a lo expuesto, en cada caso, en los antecedentes VII, VIII, IX, X, XI, XII, XIII y XIV respectivamente, de la presente resolución, por actualizarse el supuesto establecido en los artículos 113, fracción

VII y 110, fracción VII de las Leyes General y Federal de Transparencia y Acceso a la Información Pública.

Ahora bien, los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen lo siguiente:

> *"… Como información reservada podrá clasificarse aquella cuya publicación:*
>
> *[…]*
>
> ***VII.** Obstruya la prevención o persecución de los delitos;*
>
> *[…]".*

En correlación con los artículos antes mencionados, el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas, establece los parámetros para la procedencia de la causal de reserva prevista en el artículo 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública:

> *"**Vigésimo sexto**. De conformidad con el artículo 113, fracción VII de la Ley General, podrá considerarse como información reservada, **aquella que obstruya la prevención de delitos al obstaculizar las acciones implementadas por las autoridades para evitar su comisión, o menoscabar o limitar la capacidad de las autoridades para evitar la comisión de delitos.***
>
> *…".*
>
> **Énfasis añadido.**

De lo anterior se desprende, entre otras cuestiones, que podrá clasificarse como reservada aquella información que obstruya la prevención de delitos, ya sea por obstaculizar las acciones implementadas para evitar la comisión de los mismos, o bien, por menoscabar o limitar la capacidad para evitarlos.

Al respecto, cabe tener en consideración lo establecido en el documento de trabajo del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas, en el cual se define la prevención del delito de la siguiente manera: "*La prevención del delito engloba toda la labor realizada para reducir el riesgo de que se cometan delitos y sus efectos perjudiciales en las personas y la sociedad…*".

Por otro lado, las Directrices para la prevención del delito de la Organización de las Naciones Unidas enumeran tres enfoques, a saber, la prevención social, la prevención basada en la comunidad y la prevención de situaciones propicias al delito; este último tiene por objeto reducir

las oportunidades y los incentivos para delinquir, maximizar el riesgo de ser aprehendido y reducir al mínimo los beneficios del delito. En este sentido, el enfoque de prevención de situaciones está orientada en formas específicas de delincuencia.

Desde el punto de vista criminológico, prevenir es conocer con anticipación la probabilidad de una conducta criminal disponiendo de los medios necesarios para evitarla. Es decir, no permitir que alguna situación llegue a darse cuando ésta se estima inconveniente.

Ahora bien, cabe destacar que conforme a las Directrices de la Organización para la Cooperación y el Desarrollo Económico, sobre protección de la privacidad y flujos transfronterizos de datos personales, los sectores público y privado, como principio básico, deben emplear salvaguardas razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos; asimismo, se establece el principio de responsabilidad que recae sobre todo controlador de datos y su deber en el cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Asimismo, el artículo 7 del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado en Estrasburgo, Francia, el 28 de enero de 1981**,** publicado mediante Decreto de fecha 28 de septiembre de 2018 en el Diario Oficial de la Federación, establece que los Estados miembros deberán tomar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Por su parte, el artículo 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, dispone como uno de los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en dicha Ley General, contar con un sistema de supervisión y vigilancia, interna y/o externa, incluidas auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

De igual forma, de conformidad con el artículo 33, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Sujeto Obligado deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual en términos del numeral 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el responsable deberá monitorear, entre otras cuestiones, lo siguiente:

- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

De conformidad con lo anterior, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, el responsable deberá monitorear y revisar de manera periódica dichas medidas, donde no podrán pasar inadvertidas las nuevas amenazas, las posibles vulnerabilidades, los riesgos en conjunto, los incidentes y las vulneraciones de seguridad ocurridas, entre otras.

En ese sentido, el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que los sujetos obligados deben elaborar un documento de seguridad, entendiéndose como tal, el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Ahora bien, de conformidad con los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los numerales 55 al 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el documento de seguridad deberá contener, cuando menos, el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; **el análisis de riesgos, el análisis de brecha, el plan de trabajo**, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación. Dicho documento deberá actualizarse cuando se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio de nivel de riesgo; como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida; así como con la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En tal orden de ideas, el segundo párrafo del artículo 5 de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, dispone que el documento de seguridad, deberá contener las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales del Área Universitaria, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Además de lo anterior, de conformidad con el artículo 19, fracción I, incisos b) y c) de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad, durante el tratamiento automatizado de los datos personales, los sistemas de información deberán establecer las

medidas de seguridad en los periodos de inactividad o mantenimiento, así como generar respaldos y aplicar los mecanismos de control y protección para su resguardo.

Por ende, de difundirse la información contenida en los apartados relativos: **al Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades;** así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias,** se haría del conocimiento público la falta o debilidad de seguridad en un activo o grupo de activos, físicos o electrónicos, que puede ser explotada por una o más amenazas, lo que conllevaría a la materialización de las mismas y ocasionar la pérdida, destrucción no autorizada o incluso la sustracción de los datos personales en posesión de la Universidad, así como el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, además del daño, alteración o modificación no autorizada, incluso impidiendo su recuperación, vulnerando así la seguridad de los datos personales.

Bajo estos argumentos se advierte que la clasificación de la información contenida en: el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas;** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o que **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, tiene como propósito evitar o prevenir la comisión de conductas ilícitas, tales como el acceso ilícito a equipos y sistema de informática, la cual se encuentra prevista en el Título Noveno, Revelación de Secretos y Acceso Ilícito a sistemas y equipos de informática, Capítulo II, Acceso Ilícito a sistemas y equipos de informática, del Código Penal Federal en el cual se dispone lo siguiente:

> *"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa".*
>
> *"Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *…".*

De la normativa señalada se advierte que comete el **delito de acceso ilícito a sistemas y equipos de informática** todo aquel que **sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, **sean o no propiedad del Estado**, o bien, conozca o copie dicha información; conductas que de igual manera se pueden materializar en los archivos físicos, ya que es factible **sustraer, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, los datos personales contenidos en los documentos bajo custodia de las Áreas Universitarias**, por lo que la misma protección deberá otorgarse a los sistemas electrónicos, así como a los archivos físicos con los que se cuenta.

Por lo que de darse a conocer la información relativa: al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, así como a **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas**

Universitarias, la cual se encuentra contenida en los documentos de seguridad remitidos por las Áreas Universitarias, se darían a conocer las acciones implementadas o por implementar, de acuerdo con el análisis de riesgos y de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser: hardware, software, personal del responsable, manejo de documentos físicos y/o electrónicos, entre otros, lo que representa para las Áreas Universitarias un riesgo evidente para la estabilidad de la ejecución de las medidas de seguridad adoptadas para resguardar los datos en su poder, en tanto la publicación de esa información revelaría elementos que de manera concatenada con otra información que pudiera generarse o que se haya generado, evidenciaría vulnerabilidades que pudieran ser aprovechadas por personas dedicadas a la comisión de conductas ilícitas y con ello poner en riesgo la seguridad de los datos personales tratados en el desempeño y/o ejercicio de sus competencias, facultades y/o funciones.

De esta forma, se colige que con la publicidad de la información referida, se generaría un riesgo potencial tanto para la documentación física como para la infraestructura tecnológica de las Áreas Universitarias, ya que la información relativa a las medidas físicas, administrativas y técnicas puede ser utilizada para propiciar, entre otros, actos vandálicos, o bien, ataques informáticos de diversa índole, al hacerse identificables las vulnerabilidades que pueden ser explotadas y causar un daño a los documentos físicos y/o electrónicos que obran en los archivos, así como a la infraestructura informática, programas y desarrollos tecnológicos de las Áreas Universitarias, lo que limitaría severamente su capacidad para prevenir conductas ilícitas, tales como las relacionadas en párrafos anteriores.

Por lo anterior, se concluye que la información solicitada actualiza la causal de reserva prevista en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el numeral Vigésimo Sexto de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Así, en términos del artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, se analiza la siguiente prueba de daño:

> *"Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:*
>
> *I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;*
> *II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y*
> *III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio".*

I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

De difundirse la información contenida en el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades,** así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, representa un riesgo potencial para las Áreas Universitarias, pues a través de dicha información se podrían identificar vulnerabilidades que pueden ser aprovechadas para realizar conductas contrarias a derecho, tales como actos vandálicos, o bien, ataques informáticos de diversa índole, disminuyendo la capacidad de las Áreas Universitarias para responder ante posibles amenazas.

En ese sentido la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público.

II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda.

El perjuicio que en su caso ocasionaría al interés público la divulgación de la información en cuestión, supera al perjuicio que se ocasionaría al no publicarla, pues con la difusión de la información contenida en el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades,** así como **toda**

aquella información que se encuentre directamente relacionada con alguno de dichos apartados o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, se limitaría la capacidad de las Áreas Universitarias para prevenir la comisión de conductas ilícitas.

De ahí resulta evidente que el riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda.

III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

Se considera que la limitación de acceso a la información solicitada se ajusta al principio de proporcionalidad, toda vez que se justifica negar su acceso, a cambio de garantizar la capacidad de las Áreas Universitarias para implementar todas aquellas medidas y acciones tendientes a reducir el riesgo de que se cometa una conducta ilícita que pudiera vulnerar los datos personales cuyo tratamiento realizan las Áreas Universitarias, en el desempeño y/o ejercicio de sus competencias, facultades o funciones.

En ese sentido, se considera que la limitación representa el medio menos restrictivo disponible para evitar el perjuicio ya que únicamente se restringirá el acceso a la información por un periodo de **cinco años**, el cual se computará a partir de la fecha en que se emite la presente resolución y hasta la fecha de término del periodo, o bien, se interrumpirá antes si desaparecen las causas que originaron la reserva de la información, lo que suceda primero. De tal forma que no se afecte la capacidad de este sujeto obligado para prevenir la comisión de conductas ilícitas, pero tampoco se prive de manera trascendente el acceso a la información, en su momento, ya que éste no se verá restringido por un periodo mayor al previsto por la norma.

Por lo antes mencionado, se colman las hipótesis de las fracciones I, II y III, dispuestas en el artículo 104 de la Ley General de Transparencia y Acceso a la Información Pública, por lo que es procedente **CONFIRMAR** la reserva total de una parte de la información para la elaboración de la versión pública propuesta por la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** por un periodo de **cinco años**, que se computarán a partir de la fecha de la presente resolución, de conformidad con lo establecido en los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública.

CUARTA. Este Comité considera pertinente orientar a las Áreas Universitarias, a efecto de que en la elaboración de la versión pública de sus respectivos documentos de seguridad, tengan en cuenta lo siguiente:

- Deberán testar las secciones o información correspondientes al **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); a la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); a los Diagramas de Arquitectura; al Análisis de Riesgos; al Análisis de Brecha; al Plan de Trabajo; a la Política de Autenticación y Control de Acceso; a la Política de seguridad física y ambiental; a las Medidas de seguridad implementadas; a los Mecanismos de monitoreo y revisión de medidas de seguridad; a las Políticas de Respaldos; a las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados o revele vulnerabilidades en la protección de los datos personales en su poder**; para lo cual deberán emplear un medio que no permita la visualización de la misma y que no impida la lectura de aquella información que no es considerada como reservada. Al respecto, es importante precisar que **no deberán suprimirse las secciones** donde se contenga la información objeto de reserva.

- Deberán insertar un cuadro de texto en el cual se indiquen:

  - Las partes o secciones reservadas.
  - El fundamento legal que sustenta la reserva, así como el plazo de ésta, mismos que se encuentra indicados en el último párrafo de la consideración **TERCERA** de la presente resolución.

Lo anterior, de conformidad con lo dispuesto en los numerales Quincuagésimo Noveno, Sexagésimo y Sexagésimo Primero de los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas.

Por lo expuesto, y con fundamento en lo dispuesto por los artículos 6, apartado A de la Constitución Política de los Estados Unidos Mexicanos; 1, 6, 7, 8, 23, 44, fracción II, 113, fracción VII, 137 inciso a) de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 110, fracción VII, y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública; 1, 15, fracción X, 38, último párrafo del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, este Comité de Transparencia:

COMITÉ DE TRANSPARENCIA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

RESOLUCIÓN: CTUNAM/529/2022

R E S U E L V E

PRIMERO. Con fundamento en lo dispuesto en los artículos 1, 10, 11, 15 fracción X y 31, fracción I del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, 137, inciso a) de la Ley General de Transparencia y Acceso a la Información Pública y 140, fracción I de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité de Transparencia **CONFIRMA** la **CLASIFICACIÓN** de **RESERVA** total de una parte de la información, para la elaboración de la versión pública de los Documentos de Seguridad, propuesta por la **Coordinación de Servicios Administrativos Morelos,** la **Coordinación de Vinculación y Transferencia Tecnológica,** la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** la **Dirección General de Repositorios Universitarios,** la **Dirección General de Comunicación Social**, el **Instituto de Ciencias del Mar y Limnología,** la **Coordinación General de Estudios de Posgrado y la Dirección General de Asuntos Jurídicos,** en relación con: el **Inventario de sistemas de tratamiento de datos personales (rutas de acceso a soportes digitales de la información y cuentas; información técnica y operativa); la Estructura y descripción de los sistemas de tratamiento de datos personales (el tipo de soporte, la descripción y las características del lugar donde se resguardan los soportes; las rutas y los métodos de acceso a soportes digitales y físicos de la información; la URL para acceder, el tipo de sistema en el que fue desarrollado, así como el responsable de su desarrollo); los Diagramas de Arquitectura; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; la Política de Autenticación y Control de Acceso; la Política de seguridad física y ambiental; las Medidas de seguridad implementadas; los Mecanismos de monitoreo y revisión de medidas de seguridad; las Políticas de Respaldos; las Medidas de Seguridad Técnicas y aquéllas que hagan evidentes vulnerabilidades**, así como **toda aquella información que se encuentre directamente relacionada con alguno de dichos apartados** o **revele vulnerabilidades en la protección de los datos personales en poder de las Áreas Universitarias**, por un periodo de **cinco años**, contados a partir de la fecha de la presente resolución, o bien, hasta en tanto se extingan las causas que dieron origen a la reserva de la información.

Lo anterior, en términos de la consideración **TERCERA** de la presente resolución.

SEGUNDO. Se instruye a las Áreas Universitarias a efecto de que elaboren la versión pública en términos de lo dispuesto en la consideración **CUARTA.**

TERCERO. Con fundamento en los artículos 45, fracción V y 137, último párrafo de la Ley General de Transparencia y Acceso a la Información Pública: así como 53, fracción VI, inciso c) del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, notifíquese la presente resolución por correo institucional a la **Coordinación de Servicios Administrativos Morelos,** a la **Coordinación de Vinculación y Transferencia Tecnológica,** a la **Dirección General de Cómputo y Tecnologías de Información y Comunicación,** a la **Dirección General de Repositorios Universitarios,** a la **Dirección General de Comunicación Social**, al **Instituto de Ciencias del Mar y Limnología,** a la **Coordinación General de Estudios de Posgrado,** a la **Dirección General de Asuntos**

Jurídicos, así como a la Unidad de Transparencia de esta Universidad, para los efectos procedentes.

Así lo resolvió por unanimidad de votos de sus integrantes, el Comité de Transparencia de la Universidad Nacional Autónoma de México, en términos de los artículos 1, 11, 15, 20 y 53, fracción VI del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México.

POR MI RAZA HABLARÁ EL ESPÍRITU"
Ciudad Universitaria, Cd. Mx., 24 de agosto de 2022

Archivo	03-ctunam-529-2022-docto-seg-4.pdf		
Identificador único (hash)	7ea1352b88c3430d8fed8338941833551612904 0e57b16f3d4c8dadf738fabe9		
Fecha y hora de cierre	24/08/2022 19:14:12	**Fecha y hora de emisión**	24/08/2022 19:35:46
Número de páginas	42	**Firmantes**	5

Firmantes

Nombre	Lic. MARIA ELENA GARCIA MELENDEZ	**Fecha y hora de firma**	24/08/2022 16:08:25
Directora General para la Prevención y Mejora de la Gestión Institucional y Suplente del Contralor			
Hash Firma	af63b93b888bc04e10a2246f6609ccd5cf4c5136859d7432285e4b32d6301d670ca81bf6e5dd3f98e0f50ef4b5ca130f		

Nombre	Dra. Guadalupe Barrena Nájera	**Fecha y hora de firma**	24/08/2022 16:36:33
Titular de la Defensoría de los Derechos Universitarios, Igualdad y Atención de la Violencia de Género			
Hash Firma	934427d85bb1890d0ba0b7038eae904df96ad6004d5058b5cca1c8a2f887ec4bd06c8d86465ff3ff367c42f4c0684937		

Nombre	Ing. Ricardo Ramírez Ortiz	**Fecha y hora de firma**	24/08/2022 15:52:42
Director General de Servicios Generales y Movilidad			
Hash Firma	c192cd7805a02e4223fb9c95b3ff52b73d61fa338708aeccf4dda623b8f47e5b4b436deca270e424ba4eaf7dde9f6089		

Nombre	JOSE MELJEM MOCTEZUMA	**Fecha y hora de firma**	24/08/2022 17:57:01
Titular de la Unidad de Transparencia			
Hash Firma	e826eb06c8e40bfbed24f0f81ab50624c871e30f1085bd4b37991331c936ed4965a7b9b4ff85ae52896a51fc145d02ef		

Nombre	Dra. Jacqueline Peschard Mariscal	**Fecha y hora de firma**	24/08/2022 19:14:12
Especialista			
Hash Firma	155d4b30a5034a8da015b961a57db05b2ec0bf0832913877034d642ce5cd3ba748a5f504ad999eab93165beb93861fd3		